IL 5G PER RILANCIARE L'ITALIA IN SICUREZZA

RAPPORTO

TAVOLO OSSERVATORIO SULLA SICUREZZA DEL 5G

Novembre 2020

icom
istituto per la competitività

CURATORI

Silvia Compagnucci

Stefano da Empoli

Lorenzo Principali

AUTORI

Silvia Compagnucci

Thomas Osborn

Lorenzo Principali

Domenico Salerno

SI RINGRAZIANO

Laura Gagliarducci

Giulia Palocci

SOMMARIO

EXECUTIVE SUMMARY 3

1. L'IMPATTO ECONOMICO E SOCIALE DEL 5G 12

1.1. IL RUOLO DELLE RETI DURANTE LA PANDEMIA E I TREND DEL POST COVID-19 13

1.2. TECNOLOGIE, *USE CASES* E I NUOVI MODELLI DI BUSINESS 17

1.3. *VERTICALS* 5G E IMPATTO ECONOMICO IN ITALIA E IN EUROPA 20

1.4. IL *DEPLOYMENT* DELLE RETI IN EUROPA, USA E ASIA 25

2. CYBERSECURITY E 5G 30

2.1. TRA DISCRIMINAZIONE GEOGRAFICA E *RISK ASSESSMENT* 31

2.2. STRUTTURA DELLE RETI, MINACCE E MISURE PER AUMENTARE LA SICUREZZA 37

2.3. VERSO UNA STANDARDIZZAZIONE INTERNAZIONALE: SECAM, SCAS, NESAS 45

3. LA SICUREZZA DELLE RETI TRA DISCIPLINA COMUNITARIA E INIZIATIVE NAZIONALI 53

3.1. DALLA DIRETTIVA NIS, AL CYBERSECURITY ACT, AL PACCHETTO DI STRUMENTI DELL'UE PER LA SICUREZZA DELLE RETI 5G. LO STATO DELL'ARTE NELL'UNIONE EUROPEA 54

3.2. LA TUTELA DELLA SICUREZZA DELLE RETI NEI MAGGIORI PAESI EUROPEI 65

3.2.1 Germania 66

3.2.2 Spagna 68

3.2.3 Francia 70

3.2.4 Regno Unito 72

3.2.5 Strategie di scelta del vendor da parte dei maggiori operatori europei 74

4. L'ITALIA A 5G 79

4.1. STATO DELL'ARTE E PROSPETTIVE FUTURE (DESI, SPERIMENTAZIONI, INDAGINE CONOSCITIVA, OSTACOLI DI VARIA NATURA) 80

4.2. L'APPROCCIO ITALIANO ALLA SICUREZZA DELLE RETI 87

4.2.1 Il recepimento della direttiva NIS in Italia e le iniziative a tutela della sicurezza delle reti 87

4.2.2. Dal Decreto Brexit alla legge sul perimetro cibernetico. Lo stato della sicurezza informatica in Italia 92
4.2.4. La proposta di DPR per l'attività di CVCN e CV 102

CONCLUSIONI 106

EXECUTIVE SUMMARY

La permanenza forzata dei cittadini nelle proprie abitazioni causata dal Covid-19 ha avuto effetti notevoli sul sistema nazionale di telecomunicazione, determinando un aumento esponenziale del traffico dati soprattutto per via della fruizione dei contenuti di streaming video, dell'utilizzo di piattaforme videoludiche, oltre che per il massiccio ricorso da parte delle aziende allo smart working e alla formazione a distanza per gli studenti. Se diversi studi, tra cui lo stesso monitoraggio del traffico effettuato dall'Agcom, hanno mostrato chiaramente la correlazione tra l'entrata in vigore delle disposizioni atte a limitare la mobilità dei cittadini italiani e l'aumento del traffico di rete, dal punto di vista della resilienza, la rete nazionale è comunque riuscita a gestire il sovraccarico senza recare grandi disagi all'utenza. È tuttavia necessario, anche alla luce delle recenti ricadute in termini di inondamento della curva dei contagi, non rallentare lo sforzo in termini di investimenti sulle infrastrutturazioni di rete. Questo discorso appare ancor più valido in ottica 5G. L'infrastrutturazione delle nuove reti può infatti giocare un ruolo fondamentale in un orizzonte di medio-lungo termine per la ripresa nazionale dopo il crollo dovuto al Covid-19 e alle limitazioni che ne sono conseguite e che ne potrebbero ulteriormente conseguire.

Il nuovo standard di trasmissione costituisce un'importante opportunità di sviluppo e crescita a livello planetario, in particolare per la sua capacità di abilitare applicazioni avanzate proprie dell'**Internet of Things**. GSMA stima che le reti 5G porteranno un contributo all'economia mondiale di circa $ 2,2 trilioni tra il 2024 e il 2034, una crescita trainata da utilities e manifattura (33%), servizi professionali e finanziari (30%), servizi pubblici (16%), Ict e commercio (14%). Per quanto riguarda le singole aree geografiche, le stime indicano che la crescita maggiore interesserà gli Stati Uniti (oltre $ 650 miliardi), seguiti da Europa ($ 480 miliardi) e Cina ($ 460 miliardi).

L'infrastrutturazione della rete 5G quindi, oltre ad essere un **fattore abilitante** per numerose nuove tecnologie, può rappresentare un importantissimo **volano per l'economia** anche grazie agli ingenti investimenti necessari per la sua implementazione. Una stima del fabbisogno complessivo necessario in Europa per l'ammodernamento delle reti e l'implementazione delle nuove è stata effettuato da I-Com incrociando dati della Commissione Europea e del GSMA. Dall'analisi emerge un impatto di €360 miliardi necessari per il c.d. *business as usual* (manutenzione e ammodernamento), circa €155 miliardi necessari per rispettare gli obiettivi stabiliti nel quadro

della Gigabit Society e €20-30 miliardi per l'acquisizione delle licenze 5G nell'Unione Europea. Il tema degli investimenti è legato inevitabilmente al dibattito relativo alla sicurezza delle reti e, in particolare, all'opportunità di utilizzare le tecnologie dei vendor extra-europei per quanto concerne le apparecchiature, per via del possibile impatto che eventuali restrizioni potrebbero generare sugli stessi investimenti e sulla riduzione dei benefici connessi alla diffusione del 5G. L'analisi di GSMA valuta i costi di eventuali restrizioni per l'Europa in €55 miliardi, dei quali €25 miliardi derivanti dalla riduzione della concorrenza e ulteriori €30 miliardi dovuti alla sostituzione delle apparecchiature. In totale gli investimenti necessari per l'implementazione delle reti 5G in Europa sono stimati quindi in € 535 miliardi in caso di partecipazione dei fornitori extraeuropei e in € 590 miliardi in caso di esclusione degli stessi.

Per quanto concerne lo **stato di diffusione delle infrastrutture di rete mobile** nelle principali economie avanzate globali, si osserva come la Cina sia il Paese che nel 2019 ha fatto registrare la quota maggiore di infrastrutture 4G sul totale delle reti. Per quanto riguarda l'Europa, più della metà delle infrastrutture di rete mobile continentale è 4G, anche se resiste ancora una quota rilevante di connettività 2G (14%). Nello studio, GSMA effettua anche una proiezione del mix tecnologico mobile al 2025, da cui emerge come l'Europa, con il 34% di copertura 5G, sarebbe notevolmente indietro rispetto a Nord America (48%) e Cina (47%), che viaggeranno quasi di pari passo, in termini di copertura della rete di quinta generazione.

Relativamente all'attuale diffusione del 5G, I-Com ha stimato il **numero di utenti attivi** nelle principali aree sviluppate del globo. Dall'analisi emerge che il Paese che può vantare la maggior diffusione dei servizi di quinta generazione in relazione alla popolazione è la Corea del Sud (16.744 ogni 100 mila abitanti), seguita a breve distanza dalla Cina (12.790). Stati Uniti ed Europa risultano notevolmente indietro, rispettivamente con appena 2.313 e 779 utenti 5G ogni 100.000 abitanti. Lo stato attuale e la possibile evoluzione del mercato dei servizi 5G mostra quindi la necessità per l'Europa di accelerare in termini di infrastrutturazione e di offerta di servizi attrattivi per gli utenti, incrementando e favorendo gli investimenti nelle reti anche per mezzo di politiche che agevolino le attività degli operatori di settore.

Allo stesso tempo, è importante notare come il *roll-out* delle reti 5G, che risulta quanto più strategico in considerazione del potenziale spostamento, da parte di molteplici settori industriali, di una quota crescente delle proprie attività su reti di nuova generazione, stia avvenendo in un contesto in cui la **c.d. "minaccia cibernetica"** mostra una relativa stabilizzazione. I dati forniti dal

Clusit sull'evoluzione degli attacchi informatici negli ultimi sei anni, sebbene complessivamente in crescita (nel 2019 +7,6% sul 2018), in particolare per via del *Cybercrime* (i crimini informatici), presentano una sensibile diminuzione per quanto concerne la *Cyber Warfare*. A tal proposito, anche la relazione sulla politica dell'informazione per la sicurezza 2019[1], pur non fornendo i dati in termini assoluti per ragioni di riservatezza, indica come le manifestazioni "critiche" del fenomeno evidenzino un numero complessivo di azioni "ostili" quasi dimezzato rispetto al 2018, dopo il picco registrato tra il 2017 e il 2018.

Nel corso degli ultimi due anni, il dibattito relativo alla sicurezza nazionale si è focalizzato sull'opportunità o meno di utilizzare componentistica proveniente dagli operatori extra europei ed in particolare cinesi. A livello italiano, tale possibile discriminazione è ulteriormente complicata dall'**alto grado di internazionalizzazione** che si riscontra anche tra i **network providers**, in gran parte a capitale estero. Nel dettaglio, nel mercato italiano sono presenti americani e francesi tra i principali azionisti dell'ex incumbent Tim (al momento al centro della possibile transizione verso la rete unica), ancora americani in Linkem, francesi in Iliad, britannici in Vodafone, cinesi in Wind Tre e svizzeri in Fastweb.

Inoltre, per quanto concerne specificamente la **componentistica per il 5G**, si osserva come il perimetro relativo alle imprese che producono tali apparecchiature sia piuttosto ristretto, comprendendo prevalentemente Ericsson (Svezia), Nokia (Finlandia), Huawei (Cina), Samsung (Corea del Sud) e ZTE (Cina), che insieme compongono circa il 75% del mercato della fornitura di apparecchiature di rete. Tale concentrazione rende quindi piuttosto complicato attuare una discriminazione per nazionalità di provenienza dei fornitori, a fronte della previsione di misure specifiche per mitigare i rischi a 360 gradi.

A livello tecnico, sono in fase di sviluppo una **serie di misure per innalzare la sicurezza delle reti 5G**. Dall'analisi condotta emerge che due fattori, in particolare, diventeranno sempre più critici nelle evoluzioni future: **velocità e automazione**. Se è verosimile che la velocità di identificazione delle nuove minacce verrà progressivamente migliorata, la creazione di difese automatizzate per garantire la più rapida risposta possibile in caso di attacco potrebbe diventare addirittura indispensabile. Inoltre, poiché il 5G incorporerà progressivamente servizi che riguardano

[1] Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2019", febbraio 2020

direttamente la vita e il benessere dei cittadini, come la sanità e l'automotive, la sicurezza delle sue reti travalicherà il valore economico, pertanto le sue metriche trascenderanno quelle che tradizionalmente fanno capo alla sicurezza dei sistemi IT. Per tali ragioni, la sicurezza di tali reti è divenuta e diverrà sempre più una questione di interesse governativo, e potrà essere complicata dal fatto che molteplici autorità (altre nazioni, enti internazionali) vorranno imporre una serie di requisiti diversificati a diversi livelli e/o in diverse parti del mondo. Pertanto la sicurezza del 5G, in quanto standard globale, rischia di dover sottostare, oltre che ad una lunga serie di funzioni e parametri tecnici, ad un complesso e diversificato ambiente normativo.

Anche per fronteggiare la possibile tendenza alla balcanizzazione delle normative sulla sicurezza delle reti, gli operatori, già consorziati a livello mondiale dai tempi della diffusione del GSM, hanno proseguito le proprie operazioni di **standardizzazione internazionale** anche con il 3G ed il 4G, e sono al lavoro per trovare procedure comuni anche il 5G. Il 3GPP (*3rd Generation Partnership Project*), che già aveva condotto un'operazione di portata globale sul 3G, assicurando una completa interoperabilità tra le reti dei diversi operatori e nei diversi Paesi, ha introdotto la **SECAM (Security Assurance Methodology)**, un processo usato per misurare le caratteristiche relative alla sicurezza dei prodotti di rete, definendo attività e ruoli dei diversi soggetti. Il processo di valutazione SECAM comprende sia l'analisi dei processi con cui i fornitori delle apparecchiature di rete sviluppano i propri prodotti, sia la valutazione della gestione del loro ciclo di vita. A ciò si aggiunge la creazione di requisiti di sicurezza e specifiche per i test, denominate *Security Assurance Specifications* (SCAS).

Parte dei compiti di valutazione e accreditamento sono stati assegnati alla principale associazione a livello mondiale che raggruppa gli operatori di rete e i vendor, la GSM Association (GSMA). Per svolgere questi compiti, GSMA ha definito un proprio schema, il ***Network Equipment Security Assurance Scheme*** **(NESAS)**, che consiste in un insieme comune di requisiti a garanzia della sicurezza, finalizzati ad introdurre una base comune a tutti i prodotti, indipendentemente dai requisiti individuali del singolo Stato. Tali requisiti e l'intero processo di certificazione sono pensati per essere utilizzati a livello globale, lasciando che i fornitori di apparecchiature si concentrino sulla creazione e sul miglioramento del prodotto. Tra i vantaggi del NESAS si osservano la possibilità di evitare la moltiplicazione dei requisiti di sicurezza cui i fornitori dovrebbero conformare le proprie apparecchiature, il venir meno della necessità per gli operatori di rete di sviluppare specifici requisiti di sicurezza e, per i governi e le autorità nazionali, l'universale applicabilità del sistema di sicurezza e la possibilità di farlo interfacciare con le certificazioni nazionali. In questo contesto,

GSMA ha preparato una proposta da sottoporre alla Commissione europea per rendere il NESAS uno schema candidato per la certificazione del 5G.

A livello internazionale, osservando l'evoluzione delle scelte degli operatori di rete dei maggiori Paesi europei relative alla scelta dei fornitori di apparecchiature di rete 5G, si osserva come questi si stiano adeguando ai nuovi scenari complessivi del mercato. Infatti, se l'upgrade al 5G è oramai considerato un *must-have* che nessun operatore, se vuole rimanere competitivo, può permettersi di non avere, la regolamentazione europea e in particolare nazionale rappresenta un elemento che influisce sempre più nelle loro scelte.

Le posizioni di mercato sono infatti direttamente collegate alla compatibilità delle apparecchiature, ed elementi di decisiva importanza sono altresì dati dai rapporti internazionali che, in molti casi, risultano determinanti nella scelta e nel numero di fornitori ammessi in ciascun Paese. Dalla prolungata **analisi condotta sulle scelte degli operatori di rete nei 4 maggiori Paesi europei, oltre all'Italia**, si è inizialmente osservata la generale tendenza ad investire in upgrade della rete al 5G attraverso aggiornamenti delle apparecchiature preesistenti e rinnovi degli accordi con i fornitori precedenti. Tuttavia, in particolare negli ultimi mesi, in molti casi i rinnovi sono stati resi impraticabili da ragioni regolamentari, con Paesi che hanno optato per l'esclusione ex-ante dei *vendor* extra-europei per ragioni legate alla sicurezza cibernetica. Il Regno Unito, ad esempio, ha disposto la rimozione delle antenne Huawei entro il 2027, nonostante le forti perplessità degli operatori di rete nazionali, mentre in Germania il Governo ha stabilito regole più severe per tutti i *vendor* extra-UE, creando iter burocratici con criteri di sicurezza particolarmente stringenti. Una posizione simile è stata assunta anche dalla Francia che, sebbene abbia negato esclusioni ex-ante, si è riservata la possibilità di valutare autorizzazioni caso per caso per i fornitori extra-europei. Il governo spagnolo, invece, allo stato attuale non prevede l'esclusione di nessun operatore dal mercato, dando maggiore peso al raggiungimento dell'obiettivo di realizzare la copertura 5G per il 75% del territorio nazionale entro tempi molto brevi.

Dalle tendenze e dai risultati relativi alla sottoscrizione degli accordi a livello mondiale, si rileva comunque come il mercato si mantenga piuttosto ristretto con appena 4-5 fornitori che si contendono il 75% del mercato europeo. OIn tale contesto, appare certo che l'esclusione a priori di fornitori extra-europei rischi di produrre esiti problematici a livello di fornitura, con inevitabili ritardi nelle operazioni di installazione, di costi di implementazione e infine di innovazione complessiva del sistema.

Se dal punto di vista tecnologico e di mercato il tema della sicurezza appare particolarmente complesso, non meno articolato e difficoltoso l'**iter normativo che sta accompagnando il settore sia a livello comunitario che nazionale**.

Con questa consapevolezza, a livello di **Unione Europea**, l'attenzione per lo sviluppo del 5G e la creazione di un ecosistema sicuro è massima e lo dimostra l'ampia serie di iniziative messe in campo dalla Commissione negli ultimi anni. Ed infatti, il 2016 ha visto l'adozione della **direttiva NIS** (della quale è stata avviata l'attività di revisione mediante il lancio di una consultazione pubblica la cui prima fase si è conclusa il 13 agosto scorso) con la quale per la prima volta è stato definito un quadro organico della materia, affrontando le sfide in materia di cyber sicurezza e rivoluzionando la resilienza e la cooperazione in Europa, mentre il "Cybersecurity Act" del 2019 (Regolamento n. 881/2019) ha disciplinato il ruolo ed i poteri dell'ENISA, ha fissato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity ed ha istituito il Gruppo europeo per la certificazione della cybersecurity.

È sempre del 2019 la **Raccomandazione n. 2019/534 sulla cybersecurity delle reti 5G** con la quale la Commissione ha evidenziato i rischi di cybersecurity rispetto a tali reti e presentato orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi.

In attuazione di quanto previsto da tale raccomandazione, il 9 ottobre 2019 è stata pubblicata dal gruppo di cooperazione NIS una **relazione sulla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti di quinta generazione** la quale, partendo dai risultati delle valutazioni nazionali dei rischi per la cibersicurezza, effettuate da tutti gli Stati membri dell'UE, ha individuato le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici. Ad integrazione di tale rapporto degli Stati membri, il 21 novembre 2019, l'ENISA ha pubblicato un Threat Landscape for 5G Networks, in cui, sulla base anche del contributo offerto da gruppi e organismi di standardizzazione 5G e stakeholder 5G come operatori, fornitori, organizzazioni nazionali e internazionali, sono state individuate le sfide e le possibili minacce nella sicurezza delle reti 5G, è stato definito un diagramma degli asset, formulata una tassonomia delle minacce, identificata l'esposizione dei diversi asset e valutate le motivazioni dell'agente di minaccia.

Il 2020 si è aperto invece con la pubblicazione, il 29 gennaio, della Comunicazione della Commissione "***Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE***" e del pacchetto di strumenti dell'UE (**Toolbox sul 5G**) da parte del gruppo di cooperazione NIS comprendente misure di attenuazione dei rischi, che tratta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi individuando e descrivendo una otto misure strategiche ed undici tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Il 24 luglio il gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, ha pubblicato una relazione sui progressi degli Stati membri nell'attuazione del *Toolbox* sulla sicurezza 5G nella quale si fa il punto sul livello di maturità raggiunto dai vari paesi nell'implementazione delle misure contenute nel *Toolbox*. Evidenziando come tre principali rischi individuati siano quello dell'errata configurazione delle reti, della mancanza di controllo all'accesso e di interferenze statali attraverso la catena di fornitura 5G.

Il quadro normativo che si sta passo dopo passo componendo a livello comunitario è chiaramente orientato a sostenere lo sviluppo e la sicurezza delle reti 5G. Tuttavia, per garantire all'Unione la capacità di competere e giocare un ruolo da protagonista a livello globale nello sviluppo del 5G, è cruciale, da un lato, che gli Stati membri rispettino quanto più possibile la roadmap tracciata già nel 2016 dalla Commissione con l'Action Plan e, dall'altro, che a livello più generale, l'Europa persegua obiettivi di armonizzazione ambiziosi, soprattutto in materia di standard e certificazioni, che assicurino quella semplificazione e quella chiarezza indispensabili a creare un ecosistema favorevole agli investimenti ed agevolare l'operato delle aziende operanti in diversi Stati membri.

Anche l'**Italia** si trova a giocare la propria partita nello sviluppo del 5G. Se dal punto di vista della roadmap tracciata dall'Action Plan il nostro Paese si posiziona tra i primi in Europa per aver già completato le procedure di assegnazione delle frequenze destinate al 5G, più complesso e farraginoso si sta, invece, rivelando il processo di composizione del quadro normativo a garanzia della sicurezza delle reti 5G. Ed infatti, dopo che il D.L. 25 marzo 2019, n. 22 (c.d. "**Decreto Brexit**"), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41, ha esteso l'ambito applicativo dei poteri speciali (il c.d. "golden power") alle reti 5G, prevedendo l'applicazione del meccanismo di tutela dello Stato anche alle forniture di materiali e servizi, prevedendo l'obbligo di notifica in relazione a contratti o accordi aventi a oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G che vedano coinvolti soggetti esterni all'Unione europea, il 21 settembre 2019 è stato varato il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, con il quale è stato istituito il **perimetro di sicurezza nazionale**

cibernetica. Si tratta di un decreto che delinea un percorso attuativo frazionato con scadenze temporali diversificate attraverso quattro decreti del Presidente del Consiglio dei ministri ed un regolamento attraverso i quali definire, tra l'altro, le modalità e i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge, declinare i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, disciplinare le procedure di notifica degli incidenti, l'attività del CVCN e le attività di ispezione e verifica di MISE e Presidenza del Consiglio.

Il **primo DPCM (il n. 131 del 30 luglio 2020)**, dopo ampio dibattito, e dopo aver ricevuto, come da procedura delineata dal decreto legge, il parere del Consiglio di Stato e delle Camere, è stato pubblicato sulla Gazzetta Ufficiale del 21 ottobre, con ritardo rispetto alla tabella di marcia definita del decreto stesso complice, evidentemente, anche l'emergenza sanitaria in atto. Tale decreto ha individuato i criteri e le modalità per l'individuazione dei soggetti inclusi nel perimetro, ha declinato i concetti di funzione e servizio essenziale, ha selezionato i settori di attività in cui operano i soggetti da inserire nel perimetro, ha disposto l'istituzione di un Tavolo interministeriale per l'attuazione del perimetro ed ha fissato i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici.

Medio tempore, è stato proposto uno **schema di regolamento** (al vaglio del Consiglio dei Ministri), indispensabile ai fini dell'operatività del CVCN, che in attuazione del decreto istitutivo del perimetro, definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

Se il primo decreto è stato pubblicato con un ritardo di circa 7 mesi, complice, senza dubbio, anche l'emergenza sanitaria ancora in atto, e lo schema di regolamento sull'attività di CVCN e CV è ancora in fase embrionale e certamente genererà, per l'importanza delle questioni che disciplina, un ampio

dibattito, è prioritario accelerare per scongiurare il rischio che si generi un clima di generale incertezza in grado di impattare negativamente sugli investimenti e lo sviluppo delle reti 5G e di mettere a repentaglio la posizione d'avanguardia faticosamente guadagnata negli anni scorsi dal nostro Paese.

1. L'IMPATTO ECONOMICO E SOCIALE DEL 5G

1.1. IL RUOLO DELLE RETI DURANTE LA PANDEMIA E I TREND DEL POST COVID-19

Il lockdown scaturito a seguito della **pandemia di Covid-19** ha reso più evidente il ruolo nevralgico svolto dalle reti di comunicazione. Internet è diventato, ormai da alcuni anni, il centro delle attività sociali, ricreative e lavorative, nonché il canale privilegiato l'interazione di cittadini e imprese con le pubbliche amministrazioni. Nella fase di quarantena **le reti** hanno permesso a milioni di persone di lavorare, studiare, fare acquisti e mantenere i propri contatti sociali nonostante le restrizioni domiciliari.

La permanenza forzata dei cittadini nelle proprie abitazioni ha avuto però effetti notevoli sul sistema nazionale di telecomunicazione, determinando un aumento esponenziale del traffico dati, per via della fruizione dei contenuti di streaming video, dell'utilizzo di piattaforme videoludiche (prodotti ad alta intensità di dati), oltre che per il massiccio ricorso da parte delle aziende allo smart working ed alla formazione a distanza per gli studenti. Tutti questi elementi, mettendo alla prova la resilienza delle reti di telecomunicazione italiane, hanno richiesto agli operatori di **utilizzare specifiche strategie di gestione del traffico**. Fastweb, ad esempio, ha riscontrato un picco nell'utilizzo della rete fissa del 40% rispetto al periodo precedente, passando da 2,8 Terabit/s a circa 3,9 Terabit/s, mentre sia TIM che Vodafone hanno osservato un incremento dei flussi sulle reti mobili rispettivamente del 30% e del 20%. Il Milan Internet Exchange, principale snodo delle connessioni italiane da e verso l'estero – e dal quale passa il 20% del traffico italiano – ha registrato un aumento del traffico del 25% rispetto ai livelli pre-crisi. Inoltre, si è osservato inoltre un aumento di utilizzo dei *Virtual Private Network* (VPN) del 112% nella settimana tra il 9 e il 15 marzo 2020, quando molte aziende hanno deciso di far lavorare i propri dipendenti da casa.

Durante la prima ondata pandemica, l'Agcom ha effettuato un monitoraggio del traffico sulle reti di telecomunicazione (Fig.1.1) a cui hanno partecipato 24 operatori di rete fissa (pari al 99% del mercato) e 8 operatori di rete mobile (pari al 97% del mercato). Dall'analisi è emersa chiaramente la correlazione tra l'entrata in vigore delle disposizioni atte a limitare la mobilità dei cittadini italiani e l'aumento del traffico di rete. Durante il lockdown, infatti, il volume di traffico dati è aumentato del 57% su rete fissa e del 29% su rete mobile, rispetto ai valori registrati a febbraio. Parimenti il traffico voce ha visto un'impennata del 49% da fisso e del 37% da mobile. Con l'inizio della fase 2 i valori si sono lievemente ribassati, attestandosi a quota +28% su rete fissa e del +15% su rete mobile rispetto ai valori pre-emergenza (febbraio 2020). L'incremento nell'utilizzo del traffico dati

risulta ancora più evidente osservando i valori medi giornalieri, sia fissi che mobili, di petabytes transati. Il traffico medio giornaliero ha infatti sperimentato una crescita verticale dai 95/100 petabytes di gennaio e febbraio ai 147 di marzo e aprile.

Aumento del volume medio di traffico dati e voce durante la pandemia (febbraio – maggio 2020)

		Lockdown	Fase 2
Reti Fisse	Volume medio del traffico dati	+57%	+28%
	Volume medio del traffico voce	+49%	+29%
Reti mobili	Volume medio del traffico dati	+29%	+15%
	Volume medio del traffico voce	+37%	+25%

Media giornaliera traffico dati fisso e mobile durante la pandemia (Gennaio - Aprile 2020)

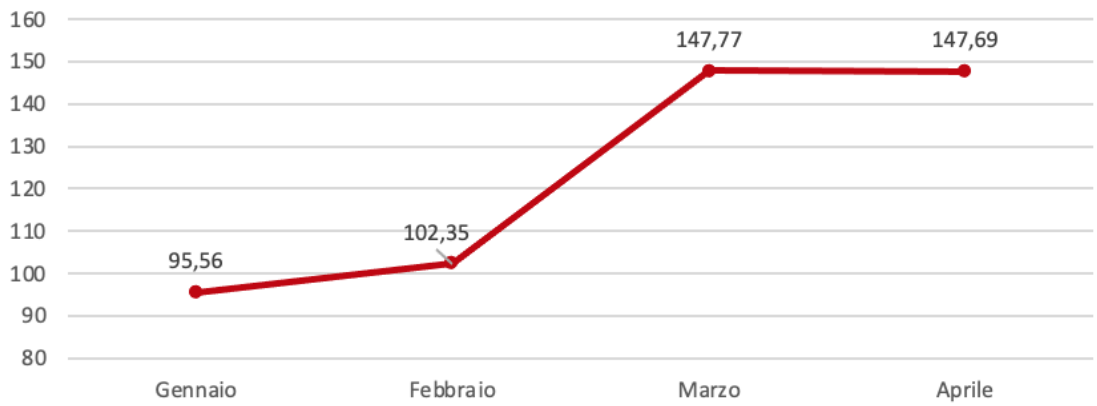

FIGURA 1.1 Rilevazioni dell'Agcom sul traffico dati e voce durante la pandemia

Fonte: Agcom

Il governo italiano, in vista del picco di connessioni generate sia da un aumento del **telelavoro** che del tempo speso dagli utenti privati su portali di streaming e piattaforme videoludiche, nel decreto Cura Italia (Art. 82 – Misure destinate agli operatori che forniscono reti e servizi di comunicazione

elettroniche) ha chiesto alle aziende del settore di adoperarsi in urgenza per potenziare le infrastrutture e **garantire la stabilità delle reti** per far fronte all'emergenza. Dal punto di vista della resilienza, la rete nazionale è comunque riuscita a gestire il sovraccarico senza recare grandi disagi all'utenza.

Secondo un'analisi effettuata da MedUX, nonostante sia stato osservato un deterioramento generale delle performance delle reti, la continuità del servizio è stata comunque ampiamente garantita. Le stime parlano, infatti, di un calo della velocità di download del 10% nelle ore di punta (h20-21) a livello nazionale (8% per i servizi FTTH) ma anche di un aumento della latenza, nei giorni di maggiore utilizzo, del 50% nelle ore del mattino e del 150% nelle ore pomeridiane. Le reti mobili hanno subìto un impatto che, sebbene inferiore a quello registrato sulle reti fisse, ha mostrato un aumento del traffico dati oscillante tra il 20% e il 30%, derivante principalmente dagli utenti "*mobile only*". Nonostante questo sia sintomo del buono stato di salute delle infrastrutture mobili italiane è necessario non rallentare lo sforzo in termini di investimenti, soprattutto in ottica 5G e tendendo in considerazioni eventuali ulteriori picchi di traffico derivanti da ulteriori limitazioni della mobilità dei cittadini. L'infrastrutturazione delle nuove reti può infatti giocare un ruolo fondamentale nel contenimento della contrazione del PIL nella auspicabile ripresa nazionale dopo il crollo dovuto al Covid-19 e alle limitazioni che ne sono conseguite e che ne potrebbero ulteriormente conseguire. A tal proposito è utile ricordare che, secondo le previsioni dell'Agcom dello scorso giugno 2020, la pandemia di Covid-19 avrebbe pesato sui ricavi del settore delle telecomunicazioni, che pure dal 2017 presentava valori in diminuzione, per un valore stimato dal 6% al 10% rispetto all'anno precedente (Fig.1.2).

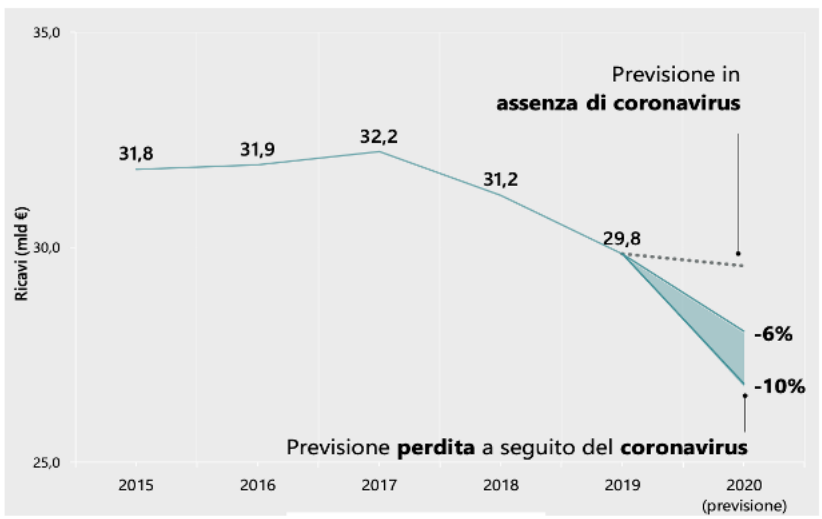

FIGURA 1.2 Previsione dei ricavi del settore delle telecomunicazioni in Italia (2015-2020)

Fonte: Agcom

La difficile situazione economica attuale e futura, unita agli stringenti vincoli normativi, rischia infatti di complicare anche il rispetto della roadmap degli obblighi di

copertura 5G. A tal proposito, secondo quanto emerso dal rapporto *"Who is prepared for the new digitale age"*, diffuso ad aprile 2020 dalla Banca Europea per gli Investimenti, lo sviluppo dell'Italia in materia di digitalizzazione è frenato in particolare da ostacoli normativi, oltre che dall'eccessiva pressione fiscale.

Anche i principali operatori del Paese, nel corso delle audizioni al Senato in vista del recepimento del Codice europeo delle comunicazioni elettroniche, hanno espresso le proprie perplessità riguardo gli eccessivi **vincoli burocratici** che stanno rallentando l'iter di ottenimento delle autorizzazioni per investire sulle infrastrutture 5G. Tra le diverse criticità, oltre alla necessità di attuare nel più breve tempo possibile la legge sul perimetro di sicurezza nazionale cibernetica, si è posto l'accento sull'importanza di uniformare la normativa italiana sulle emissioni a quella dell'Unione Europea e sulla semplificazione delle norme che regolano interventi e installazioni, non sempre omogenee su tutto il territorio nazionale, al fine di evitare l'insorgere di gap tecnologici tra un'area e l'altra del Paese.

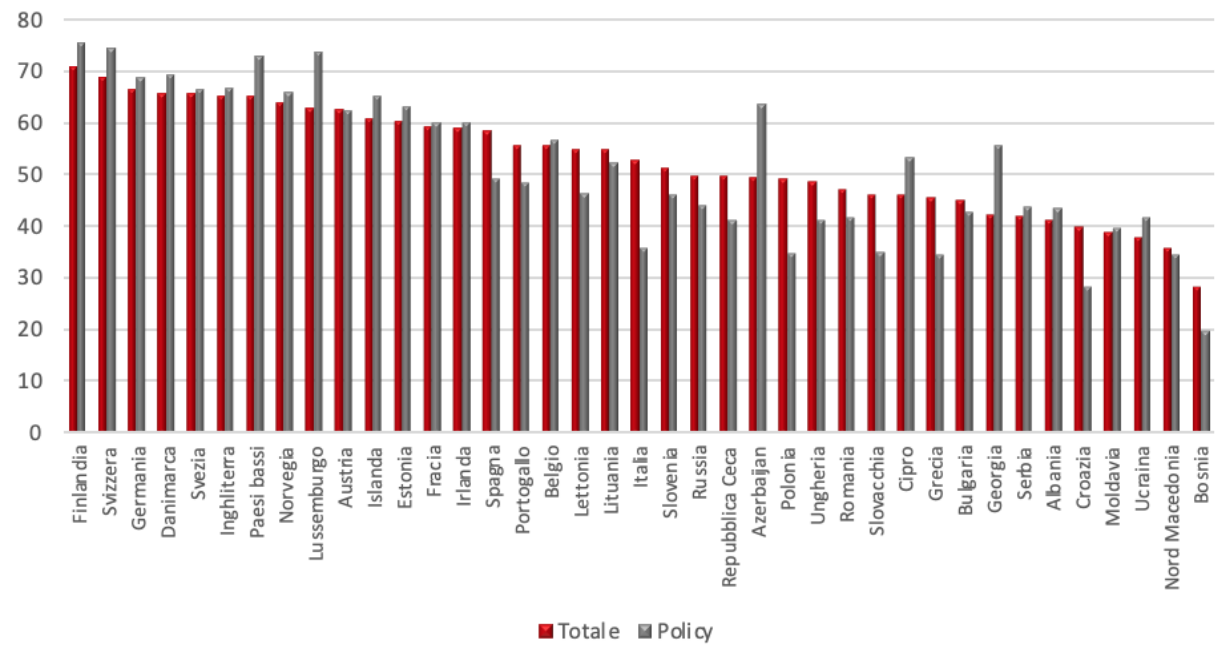

FIGURA 1.3 5G Readiness Index (2020)

Fonte: *Europe 5G Readiness Index Report, inCITES Consulting*

1.2. TECNOLOGIE, *USE CASES* E I NUOVI MODELLI DI BUSINESS

Il nuovo standard di trasmissione di quinta generazione costituisce un'importante opportunità di sviluppo e crescita a livello planetario, in particolare per la sua capacità di **abilitare applicazioni avanzate proprie dell'*Internet of Things***. A livello tecnico, il 5G può garantire una velocità di trasferimento dei dati fino a 10 Gbps (100 volte più veloce dell'LTE), ridurre la latenza fino ad 1 millisecondo, consentire di gestire un milione di dispositivi in 1 km^2 e assicurare una maggiore longevità della batteria dei dispositivi. Il 5G ha le potenzialità per ridisegnare i servizi di connettività di tipo fisso (*wireless last mile* ad altissima capacità) e di tipo mobile (altissimi volumi di dati), abilitando la diffusione pervasiva di oggetti che avranno la capacità di interagire tra di loro e con l'uomo condividendo le conoscenze acquisite.

I cluster applicativi in cui sarà più evidente l'impatto della nuova tecnologia – che come anticipato fanno capo all'Internet delle cose – utilizzeranno prevalentemente **tre funzioni**, ovvero *Massive Machine-type*, *Critical Machine-type* e *Enhanced Mobile Broadband* (e-MBB), che definiranno il ruolo del 5G in qualità di acceleratore per la trasformazione digitale delle aziende e abiliteranno lo sviluppo di nuovi servizi avanzati. Nel cluster degli *use-case IoT Massive Machine-type* rientrano tutte le reti di sensori, contatori intelligenti, rilevatori per il monitoraggio remoto di asset strategici e strutture, con requisiti chiave in termini di durata della batteria, densità di connessione supportata, affidabilità del servizio, e senza SLA particolarmente sfidanti in termini di latenza e mobilità.

Negli *use-case IoT Mission Critical Machine-Type*, invece, si annoverano tutte quelle applicazioni che necessitano di performance particolarmente elevate in termini di affidabilità del servizio (99,99%), di latenza (~ inferiore ai 10ms) e di mobilità (anche superiore ai 500Km/h). Si pensi, ad esempio, al telecontrollo remoto di smart grid con requisiti di 8ms di latenza oppure, servizi IoT per treni ad alta velocità, con requisiti di mobilità di + 500 Km/h e latenza inferiore a 10 millisecondi, fino a servizi sanitari avanzati come la chirurgia da remoto ed il monitoraggio a distanza dello stato di salute dei pazienti (meno di 1ms di latenza e affidabilità stimata del 99,999%).

Tra i servizi avanzati appartenenti alla categoria dell'*Enhanced Mobile Broadband,* infine, rientrano tutte quelle applicazioni che prevedono tipicamente come requisiti chiave di supportare un throughput estremamente elevato (anche +10Gbps) e una latenza inferiore ai 5 millisecondi, fornendo al tempo stesso servizi affidabili, di qualità e altamente efficienti (si tratta, in particolare,

di servizi legati all'offerta di esperienze avanzate di intrattenimento, video e automazione domestica come esperienze immersive di gaming, e-learning e remote-training etc.). La piena espressione delle potenzialità dei cluster *IoT Critical Machine-type* e dei servizi in *Enhanced Mobile Broadband* esigono lo sviluppo delle piattaforme 5G capaci di abilitare i requisiti essenziali per la loro applicazione in termini di latenza, user throughput, mobilità, densità di traffico, affidabilità del servizio e sicurezza. I settori maggiormente impattati a livello economico, e che potrebbero vedere la nascita delle applicazioni maggiormente innovative, sono attualmente l'automotive, i trasporti, l'energia, la sanità e la manifattura.

Secondo un'analisi condotta da DLA Piper[2] nel corso del primo trimestre del 2020 (Fig.1.4), l'applicazione del 5G con il più alto potenziale di crescita nel prossimo futuro è relativa alle **smart cities** (22%), seguita dall'IoT (16%) e dal Media & entertainment (16%). Al comparto smart cities e 5G afferiscono le applicazioni che vanno dal monitoraggio della qualità dell'aria, dell'uso dell'energia e dei modelli di traffico all'illuminazione stradale, ai sistemi di parcheggio intelligente, alla gestione dei flussi di moltitudini di persone e alla risposta alle emergenze. Osservando la classifica risulta evidente come la maggior parte dei rispondenti al sondaggio prediliga **settori in cui la tecnologia appare già pronta all'ingresso del 5G**, mentre viene ritenuto inferiore il potenziale

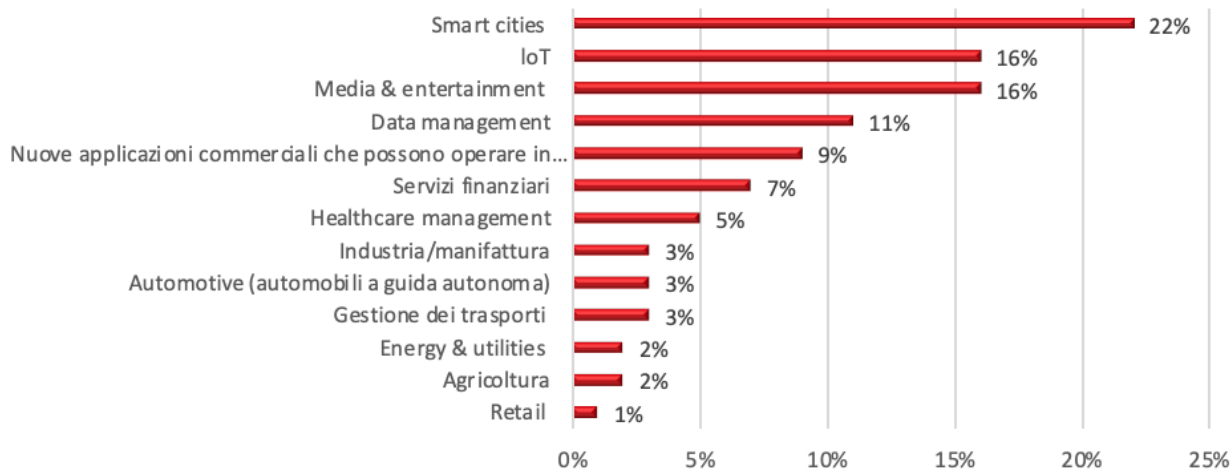

FIGURA 1.4 Use case del 5G con il maggior potenziale di crescita in Europa (2020)

Fonte: DLA Piper

[2] Lo studio è stato condotto intervistando 235 esperti di tecnologia provenienti sia dal mondo dell'impresa che dalle pubbliche amministrazioni Europee.

di crescita di applicazioni avanzate come l'auto a guida autonoma, rivoluzionarie in prospettiva ma ancora non pronte ad esordire sul mercato.

Qualcomm ha effettuato nel 2017 uno studio[3] per identificare le caratteristiche del 5G eMBB più attrattive per i consumatori. L'interesse dei partecipanti allo studio è stato attratto in particolare dalla possibilità di abbandonare l'utilizzo del wifi pubblico in mobilità (48%) e dal poter avere a disposizione una rete super veloce (48%). Altri aspetti rilevanti hanno riguardato la possibilità di accedere ai propri file in cloud all'istante (21%) e di poter effettuare lo streaming di video ad altissima risoluzione potendo così sfruttare a pieno le potenzialità degli ultimi smartphone in commercio.

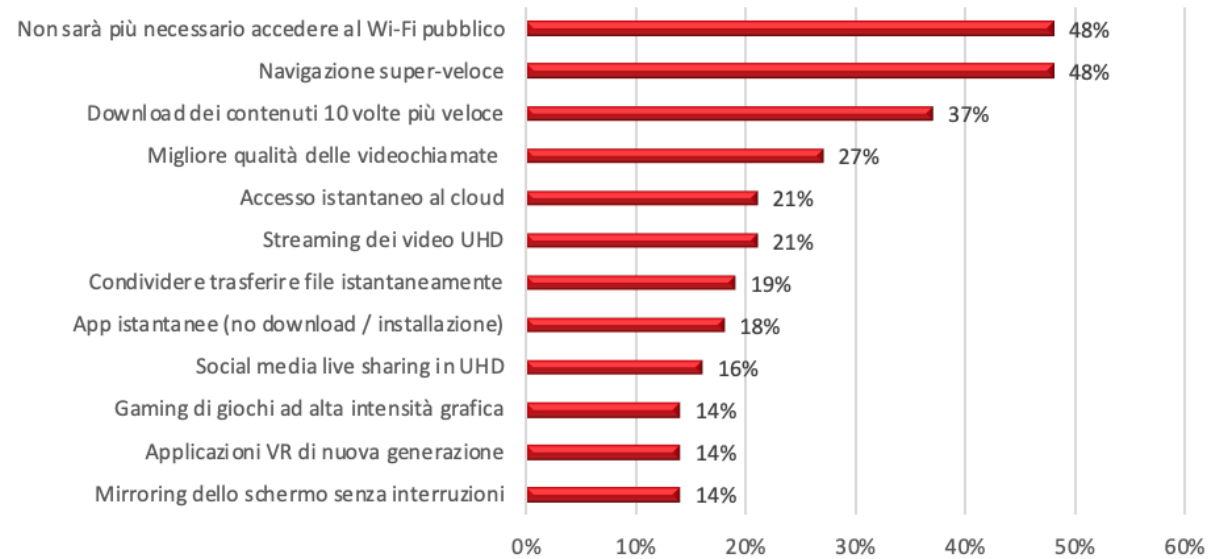

FIGURA 1.5 Applicazioni 5G eMBB più attrattive per i consumatori (2017)

Fonte: Note: Le percentuali superano il 100% perché era possibile esprimere più di una preferenza

Fonte: GSMA, 2020

In generale, quindi, il favore degli utenti potenziali rispetto alle applicazioni di nuova generazione appare prevalentemente **rivolto a servizi disponibili e utilizzabili già nel breve periodo**.

[3] All'indagine hanno partecipato 5844 possessori di smartphone provenienti da 6 Paesi (USA, Cina, UK, Francia, Germania e Finlandia)

1.3. *VERTICALS* 5G E IMPATTO ECONOMICO IN ITALIA E IN EUROPA

Come anticipato nel paragrafo precedente, l'evoluzione tecnologica del 5G consentirà lo sviluppo di applicazioni e servizi altamente innovativi in molteplici settori industriali. Nel corso dell'ultimo decennio numerosi studi hanno provato a stimare l'impatto dell'introduzione delle reti di quinta generazione sull'economia globale. Affinché una proiezione di questo tipo risulti realizzabile è però necessario che l'implementazione delle reti e lo sviluppo delle tecnologie ad essa applicate seguano la *time-line* preventivata nel momento in cui lo studio è stato redatto. Sfortunatamente **non sempre il *deployment* di una tecnologia segue un percorso lineare**, trovandosi spesso frenato da problemi di natura burocratica, come nel caso del 5G, e/o di natura tecnica (ad esempio l'auto a guida autonoma). In questo paragrafo viene effettuata una disamina dei principali studi al fine di offrire al lettore una panoramica quanto più completa possibile sulla tematica di rifermento.

GSMA, nello studio *"Mobile Economy Report 2020"* pubblicato nel marzo 2020, prevede **che le reti 5G porteranno un contributo all'economia mondiale di circa $ 2,2 trilioni tra il 2024 e il 2034**. I settori che traineranno questa crescita (Fig.1.6) sono: utilities e manifattura (33%); servizi professionali e finanziari (30%); servizi pubblici (16%); Ict e commercio (14%); agricoltura e settore minerario (6%).

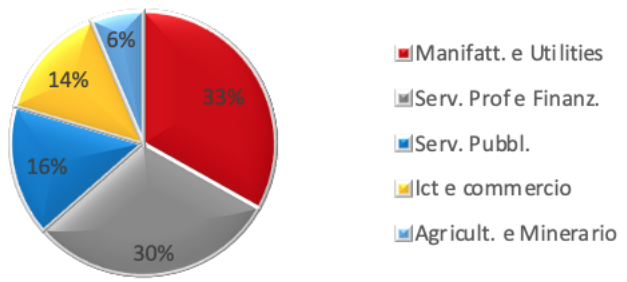

FIGURA 1.6 Contributo previsto del 5G alla crescita economica globale per settore (%, 2034)
Fonte: GSMA, 2020

Per quanto riguarda le singole **aree geografiche** (Fig.1.7) le stime indicano che la crescita maggiore interesserà gli Stati Uniti (oltre $ 650 miliardi), seguiti da Europa ($ 480 miliardi) e Cina ($ 460 miliardi). Nel 2034 la Cina potrebbe ricevere molti più benefici da manifattura e utilities (fino a $ 270 miliardi) mentre Usa ed Europa vedrebbero crescere i ricavi da servizi professionali e finanziari rispettivamente fino a $ 250 e $ 170 miliardi. A livello di servizi pubblici l'Europa potrebbe generare benefici fino a 3 volte superiori a quelli della Cina ($ 90 vs $ 30 miliardi) ma comunque sensibilmente inferiori agli Usa (circa $ 150 miliardi).

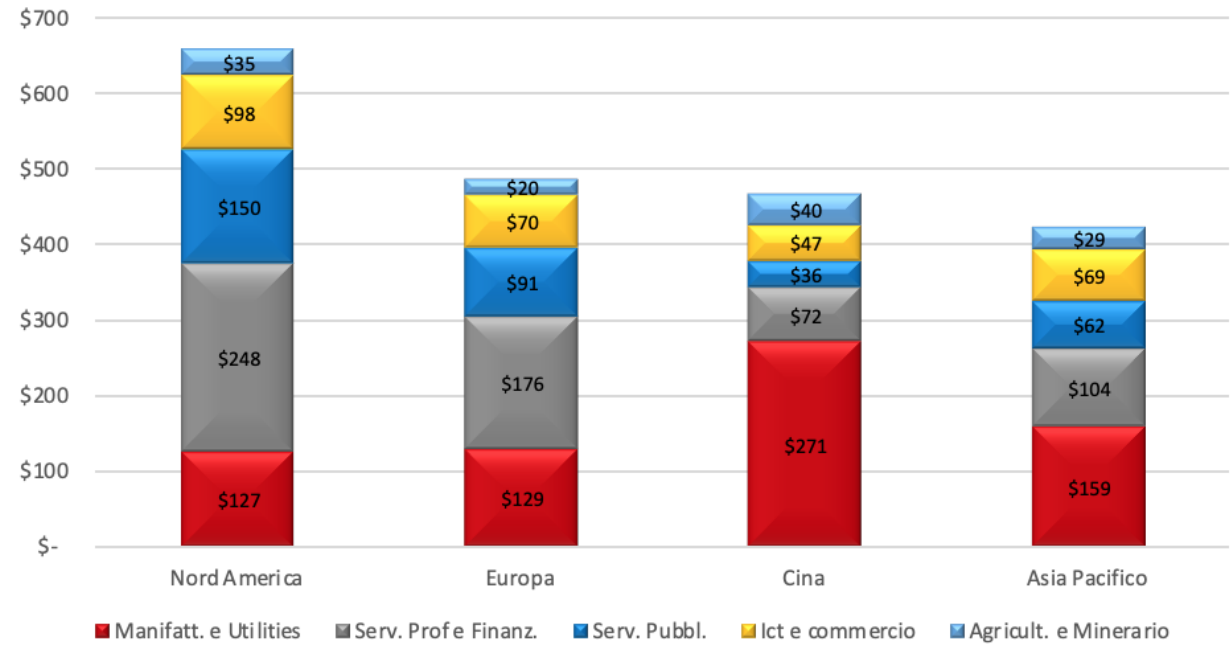

FIGURA 1.7 Contributo del 5G alla crescita economica globale per area geografica e settore (in miliardi di $, 2034)

Fonte: GSMA, 2020

Sempre in relazione alle stime di impatto al 2034, una parte rilevante della crescita imputabile al 5G potrebbe essere raggiunta grazie all'utilizzo delle ***mmWave*** (onde millimetriche) ovvero la porzione di spettro che va dai 24 GHz agli 86 GHz. L'utilizzo di queste frequenze consente di sfruttare canali di comunicazioni molto più ampi rispetto alle bande minori, garantendo quindi maggiori velocità di trasferimento dati e minore latenza. Per questo motivo l'entrata in servizio delle *mmWave* è ritenuta dal GSMA un tassello fondamentale al fine di sfruttare a pieno le potenzialità del 5G.

Dal punto di vista economico (Fig. 1.8), entro il 2034 l'utilizzo delle onde millimetriche dovrebbe portare benefici complessivi per $565 miliardi a livello globale. Le applicazioni che si prevede generino il maggior contributo sono l'automazione industriale, in controllo da remoto dei dispositivi e la realtà virtuale. A livello settoriale, le stime indicano che i maggiori benefici

dovrebbero provenire dalla manifattura e dalle utilities ($215 miliardi), dai servizi professionali e finanziari ($141 miliardi) e dai servizi pubblici ($96 miliardi).

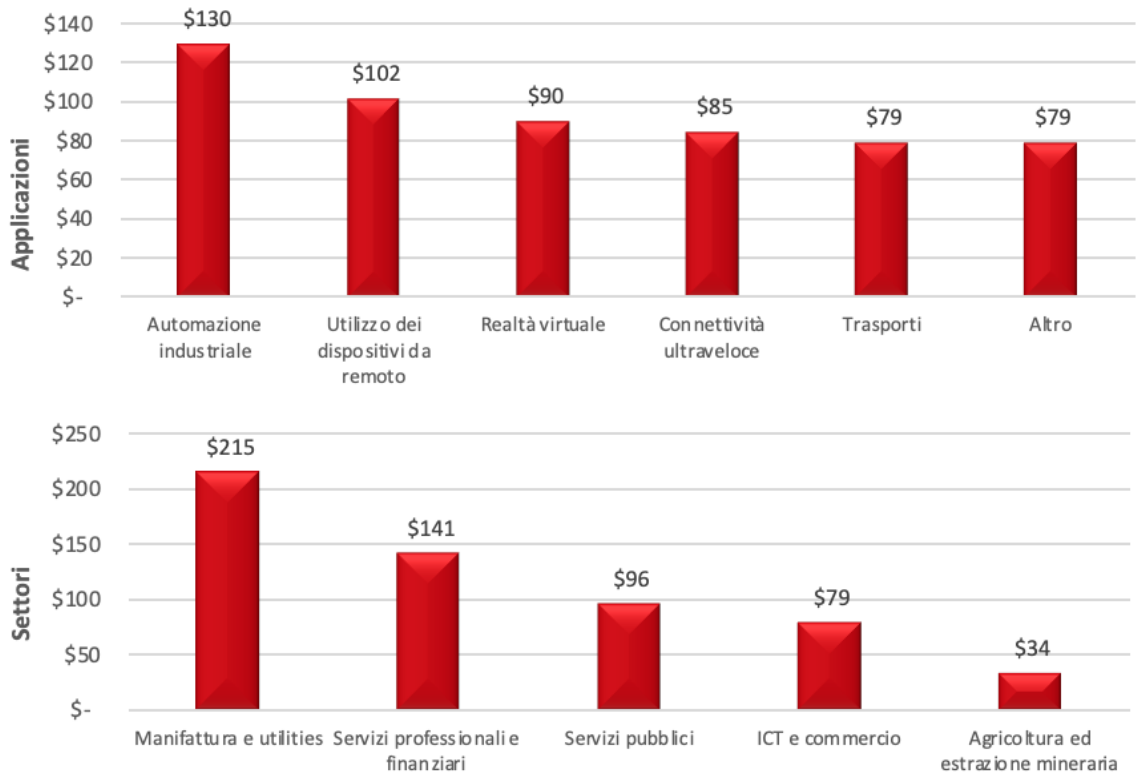

FIGURA 1.8 Impatto economico dell'utilizzo delle onde *mmWave* nel 2034 a livello globale (miliardi di dollari)

Fonte: Elaborazioni I-Com su dati GSMA

Lo studio supportato dalla **Commissione Europea** del 2016, *"Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe"* ha invece stimato che la diffusione del 5G avrebbe determinato **benefici economici**, derivanti dai **4 principali verticals** (automotive, sanità, trasporti ed energia), per € 141,7 miliardi di euro già nel 2020. L'analisi, effettuata da una serie di istituti di ricerca per conto della Commissione[4], ha cercato di stimare il moltiplicatore degli investimenti in 5G (programmati entro il 2020) e il loro effetto sul mercato del lavoro. Sfortunatamente, a 4 anni di distanza dalla pubblicazione dello studio, la quota

[4] Trinity College, Tech4i2, Real Wireless and InterDigital

di investimenti pervista, che nel caso dell'Italia ammontava a 6,8 miliardi di euro, sembra ancora lontana dall'essere raggiunta (salvo quanto messo a bilancio dagli operatori per le licenze 5G). Nonostante ciò, la ricerca può essere utilizzata come una stima della perdita economica e di posti di lavoro derivante dal non aver rispettato la tabella di marcia preventivata nel 2016 nel rollout delle reti di nuova generazione (Fig.1.9).

	Investimenti in 5G	Effetto moltiplicatore	Posti di lavoro creati
Austria	970 €	2.170 €	25.200
Belgio	1.230 €	3.150 €	36.300
Bulgaria	840 €	2.320 €	128.900
Croazia	480 €	1.540 €	64.400
Cipro	100 €	470 €	20.800
Repubblica ceca	1.200 €	3.990 €	143.000
Danimarca	620 €	1.480 €	14.800
Estonia	150 €	560 €	13.600
Finlandia	600 €	1.501 €	19.900
Francia	7.030 €	17.110 €	224.700
Germania	9.280 €	20.740 €	211.100
Grecia	1.220 €	2.180 €	101.300
Ungheria	1.130 €	3.450 €	134.600
Irlanda	490 €	1.210 €	10.700
Italia	6.830 €	15.700 €	186.830
Lettonia	230 €	570 €	16.800
Lituania	330 €	700 €	28.200
Lussemburgo	60 €	122 €	600
Malta	50 €	190 €	3.900
Olanda	1.870 €	5.030 €	68.300
Polonia	4.350 €	13.040 €	569.553
Portogallo	1.170 €	3.730 €	127.300
Romania	2.270 €	4.660 €	252.300
Slovacchia	620 €	1.980 €	71.500
Slovenia	240 €	610 €	14.700
Spagna	5.190 €	14.600 €	329.400
Svezia	1.060 €	2.450 €	25.300
UK	7.040 €	16.520 €	172.100

FIGURA 1.9 Stima dell'impatto economico e sul mercato del lavoro degli investimenti per il 5G al 2020 (2016)

Fonte: Commissione europea

Sulla base di queste stime, dunque, i mancanti investimenti nel 5G avrebbero prodotto benefici economici fino a **€15,7 miliardi e fino a 186 mila posti di lavoro**. L'infrastrutturazione della rete 5G quindi, oltre ad essere un fattore abilitante per numerose nuove tecnologie, può rappresentare un importantissimo **volano per l'economia** anche grazie agli importanti investimenti necessari per la sua implementazione. Una stima del fabbisogno complessivo necessario in Europa per l'ammodernamento delle reti e l'implementazione delle nuove è stata effettuato da I-Com incrociando dati della Commissione europea e del GSMA (Fig.1.10). Dall'analisi emerge un impatto di €360 miliardi necessari per il c.d. business as usual (manutenzione e ammodernamento), circa €155 miliardi necessari per rispettare gli obiettivi stabiliti nel quadro della ***Gigabit Society***[5] (tra cui €98 miliardi per portare la connettività ultra broadband nelle aree rurali, €35 miliardi per coprire driver socioeconomici quali scuole, università e ospedali e 22 miliardi per la connessione ad altissima velocità delle direttrici di trasporto) e €20-30 miliardi per l'acquisizione delle licenze 5G nell'Unione Europea.

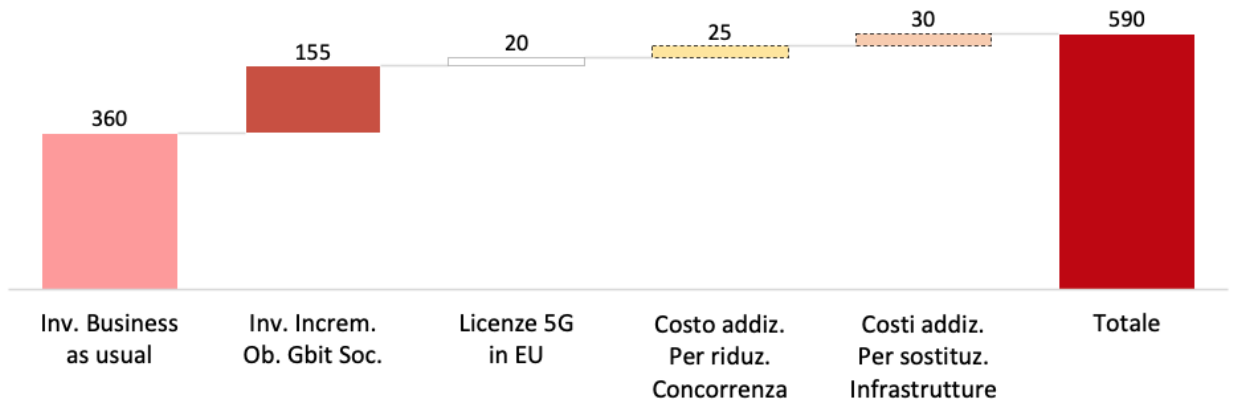

FIGURA 1.10 Stima investimenti necessari per l'implementazione delle reti 5G in Europa (in € mld, 2019-2025)

Fonte: Note: Le figure tratteggiate si riferiscono ai costi addizionali derivanti dall'esclusione dei fornitori extraeuropei
Fonte: elaborazioni I-Com su dati Commissione Europea e GSMA

Il tema degli investimenti è legato inevitabilmente al dibattito relativo alla **sicurezza delle reti** e, in particolare, all'opportunità di utilizzare le tecnologie dei **vendor extra-europei** per quanto concerne le apparecchiature di rete, per via del possibile impatto che eventuali restrizioni

[5] COM(2016) 587 del 14.9.2016 "Connettività per un mercato unico digitale competitivo: verso una società dei Gigabit europea"

potrebbero generare sugli stessi investimenti e sulla riduzione dei benefici connessi alla diffusione del 5G. L'analisi di GSMA valuta i costi di eventuali restrizioni per l'Europa in €55 miliardi, dei quali €25 miliardi derivanti dalla riduzione della concorrenza e ulteriori €30 miliardi dovuti alla sostituzione delle apparecchiature. In totale gli investimenti necessari per l'implementazione delle reti 5G in Europa sono stimati quindi in € 535 miliardi in caso di partecipazione dei fornitori extraeuropei e in € 590 miliardi in caso di esclusione degli stessi. Si rileva quindi l'importanza di valutare in modo appropriato il *trade-off* tra costi e benefici che gli interventi normativi in tema di cibersicurezza potrebbero determinare nel sistema-Paese.

1.4. IL *DEPLOYMENT* DELLE RETI IN EUROPA, USA E ASIA

Il livello di avanzamento tecnologico di un Paese è da sempre direttamente correlato con il grado di **sviluppo delle sue infrastrutture**. Con l'avvento dell'era digitale lo sviluppo delle reti è diventato un volano di crescita economica e sociale. In questo paragrafo viene analizzato il grado di sviluppo delle infrastrutture di rete europee a confronto con quello delle altre principali aree maggiormente sviluppate del pianeta. A tal proposito, GSMA pubblica annualmente un indice che valuta il **livello della connettività** mobile di un Paese, il "*GSMA Mobile Connectivity Index*", basato sullo stato di quattro variabili[6] tra cui lo stato delle infrastrutture. Osservando i punteggi assegnati all'ambito infrastrutturale (Fig.1.11) si osserva come il valore medio dei Paesi appartenenti all'UE27 (78,0) risulti inferiore a quello del Giappone (83,4), della Corea del Sud (80,8) e degli Stati Uniti (79,9). Tra le aree considerate, l'unica che presenta un valore inferiore a quello europeo è la Cina (76,0).

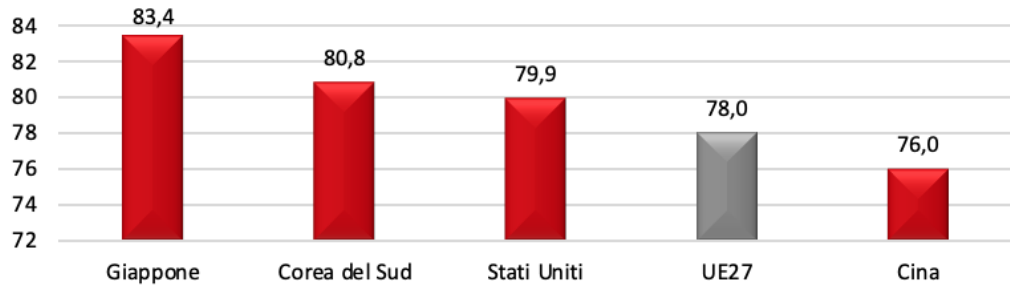

FIGURA 1.11 GSMA Mobile Connectivity Index 2020 ambito infrastrutture

Fonte: Elaborazioni I-Com su dati GSMA 2020

[6] Variabili considerate nel GSMA Mobile Connectivity Index: Infrastrutture; Accessibilità; Prontezza dei consumatori; Contenuti e servizi.

Nonostante quest'ultima occupi l'ultimo posto tra le aree avanzate nella classifica infrastrutturale dell'indice, osservando i dati sul mix tecnologico nelle reti mobili pubblicati dallo stesso GSMA, emerge come il Paese asiatico sia quello che nel 2019 aveva la quota maggiore di infrastrutture 4G sul totale delle reti (Fig.1.12).

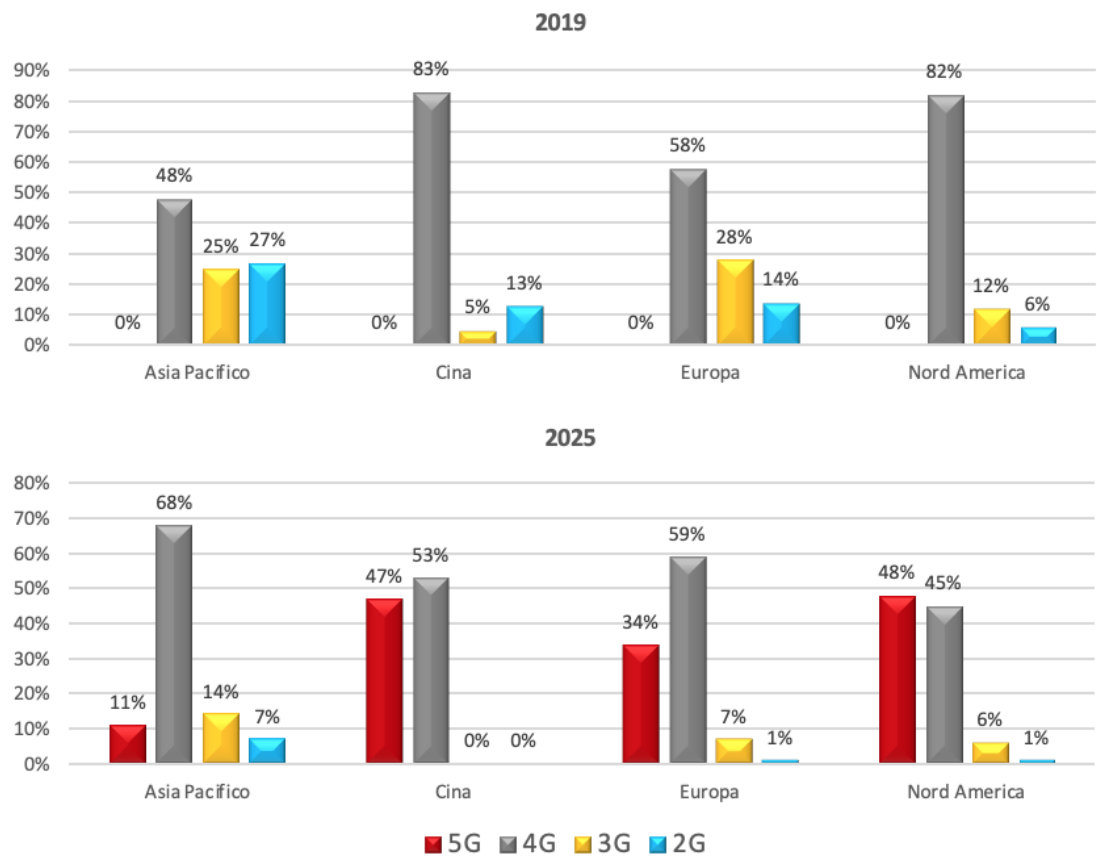

FIGURA 1.12 Mix tecnologico delle reti mobili per area geografica (2019 – stime 2025)

Fonte: GSMA, 2020

Per quanto concerne l'Europa, più della metà delle infrastrutture di rete mobile continentale è 4G, anche se resiste ancora una quota rilevante di connettività 2G (14%). Nello studio, GSMA effettua anche una proiezione del mix tecnologico mobile al 2025, da cui emerge come l'Europa, con il 34% di copertura 5G, sarebbe notevolmente indietro rispetto a Nord America (48%) e Cina (47%), che viaggeranno quasi di pari passo, in termini di copertura della rete di quinta generazione.

Per quanto concerne le **bande di frequenza prioritarie** selezionate nelle varie **aree geografiche** (Fig.1.13) risulta evidente dalla mappa sottostante (diffusa da GSMA) come gli Stati Uniti siano il Paese che ha destinato alle reti di quinta generazione la porzione di spettro più ampia, selezionando 7 bande che vanno dai 600 MHz fino ai 71 GHz. Le altre aree considerate hanno selezionato tutte 3 porzioni di spettro seppur con delle sostanziali differenze. L'Europa è l'unica, oltre agli Stati Uniti, ad aver selezionato una banda sotto i 3 GHz (700 MHz), una intermedia (3,4-3,8 GHz) e una millimetrica (26 GHz). Il Giappone ha invece selezionato 2 bande intermedie (3,6-4,2 GHz e 4,4-4,9 GHz) e una millimetrica (28 GHz) al contrario della Corea del Sud che ha scelto 2 mmWave (26 e 28 GHZ) e una media (3,4-3,7 GHz). La Cina si distingue per essere l'unico Paese ad aver selezionato esclusivamente bande intermedie (3,3-3,4 GHz, 3,4-3,6 GHz e 4,8- 5 GHz).

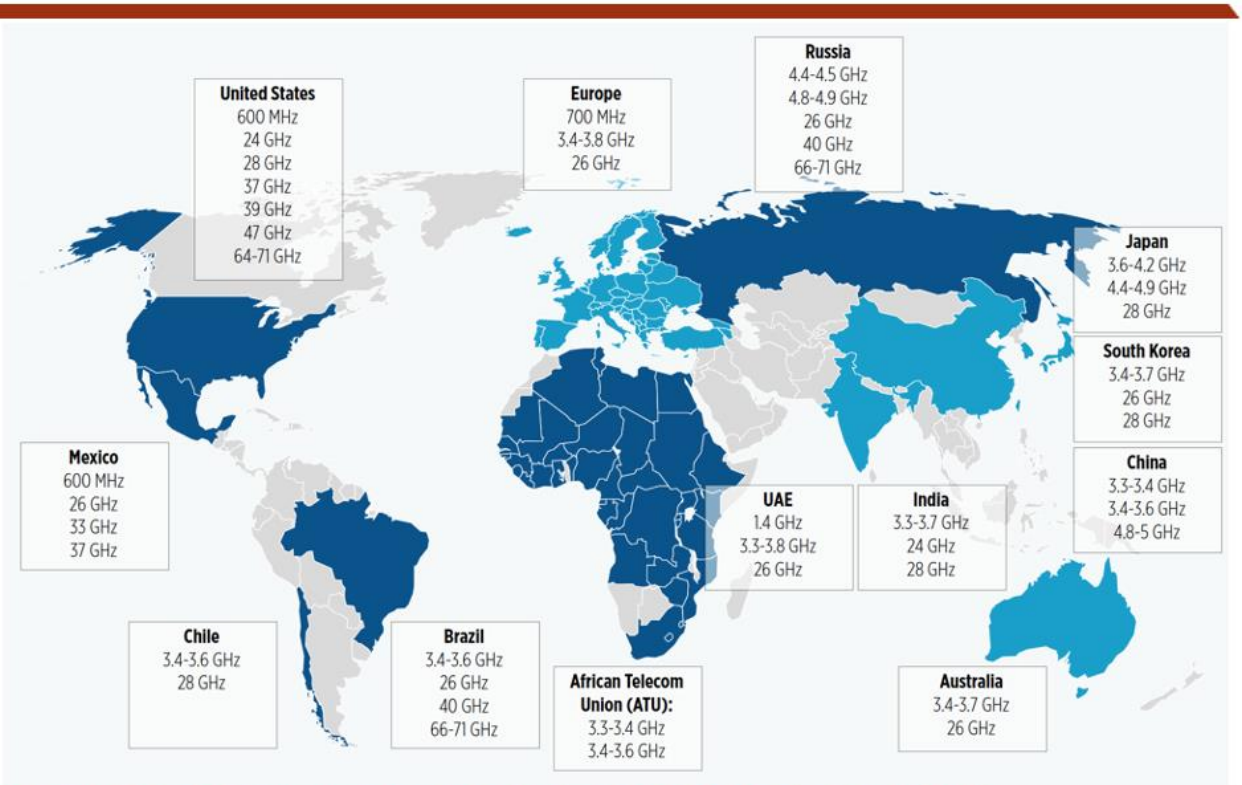

FIGURA 1.13 Bande di frequenza prioritarie selezionate per il 5G a livello globale (2020)

Fonte: GSMA

L'ultimo report del 5G Observatory (settembre 2020) evidenzia come in **Europa** negli ultimi due anni siano stati effettuati una serie di passi in avanti in ambito 5G, tra cui il **lancio del servizio**

commerciale da parte di molteplici operatori (Fig.1.14), l'arrivo sul mercato dei primi smartphone compatibili e la diffusione di numerose base station nelle maggiori città europee. Per quanto concerne i servizi commerciali 5G, questi risultano attualmente disponibili in 19 Paesi europei (incluso il Regno Unito)[7].

Negli Stati Uniti il lancio del primo servizio commerciale 5G è stato operato ad ottobre 2018 da Verizon, che ha offerto ai residenti di 4 città (Houston, Sacramento, Indianapolis e Los Angeles) la possibilità di connettersi in FWA sfruttando lo standard di quinta generazione. Il primo operatore USA a lanciare il servizio 5G per utenti mobili, nel dicembre 2018, è stato invece AT&T utilizzando le frequenze a 39 GHz. Il lancio commerciale del 5G in Corea del Sud è invece avvenuto nel dicembre 2018 per i clienti aziendali e nell'aprile 2019 per gli utenti residenziali. I tre maggiori operatori cinesi (China Mobile, China Telecom e China Unicom) hanno lanciato i primi servizi 5G in contemporanea il 1° novembre 2019 in 50 città del Paese. Il Giappone è stato l'ultima tra le aree considerate ad aver lanciato servizi commerciali su rete di quinta generazione ad aprile 2020.

FIGURA 1.14 Lancio dei servizi 5G a livello mondiale

Fonte: 5G Observatory, settembre 2020

Nonostante sia difficile fornire una cifra esatta degli utilizzatori di servizi 5G, data la recente messa in opera dei servizi e la scarsità di dati forniti dagli operatori, I-Com ha stimato il **numero di utenti attivi ogni 100.000 abitanti** utilizzando dati provenienti da molteplici fonti primarie (Fig.1.15).

[7] Questi sono Austria, Belgio, Bulgaria, Danimarca, Finlandia, Germania, Ungheria, Irlanda, Italia, Lettonia, Paesi Bassi, Polonia, Repubblica ceca, Romania, Slovenia, Spagna, Svezia, Ungheria e Regno Unito.

Dall'analisi emerge che il Paese che può vantare la maggior diffusione dei servizi di quinta generazione in relazione alla popolazione è la Corea del Sud[8] (16.744 ogni 100 mila abitanti), seguita a breve distanza dalla Cina (12.790). Stati Uniti ed Europa, in base ai dati emersi, risultano notevolmente indietro ai primi due Paesi esaminati, con rispettivamente appena 2.313 e 779 utenti 5G ogni 100.000 abitanti. Il Giappone con 190 utenti figura all'ultimo posto tra le aree considerate, anche se occorre considerare che il Paese asiatico è l'ultimo in ordine di tempo ad aver lanciato servizi commerciali 5G e che, tra gli operatori mobili giapponesi, solo uno ha reso disponibili i dati ufficiali relativi ai propri utenti.

Nel complesso, dunque, si osserva la necessità per l'Europa di accelerare in termini di infrastrutturazione e di offerta di servizi attrattivi per gli utenti, incrementando e favorendo gli investimenti nelle reti anche per mezzo di politiche che agevolino le attività degli operatori di settore.

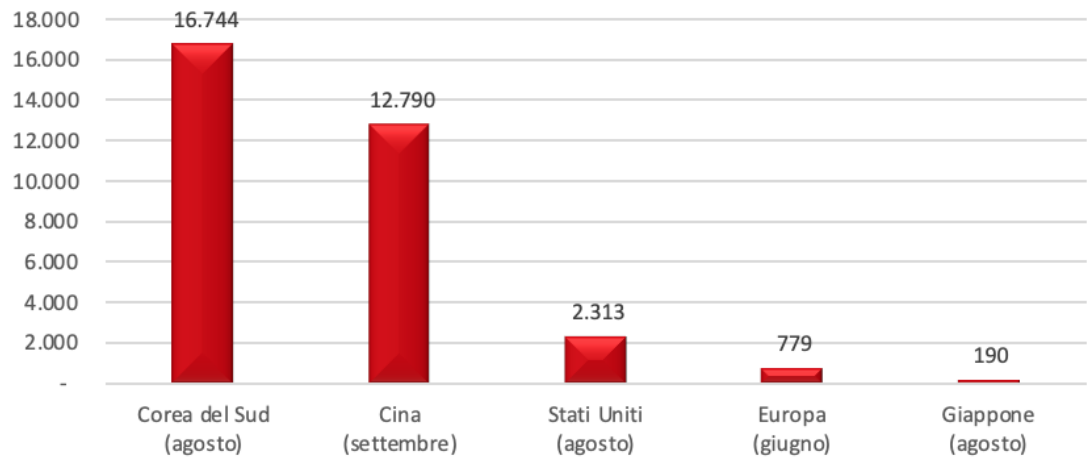

FIGURA 1.15 Utenti 5G per area geografica (per 100.000 abitanti, 2020)

Note: Alcuni operatori (Unicom – China, KDDI – Giappone, SoftBank – Giappone) non hanno rilasciato dati sul numero di utenze 5G sottoscritte. Il dato degli Stati Uniti è relativo al numero di terminali 5G venduti dagli operatori.
Fonte: Elaborazioni I-Com su dati Ministero della scienza e dell'ICT della Corea del Sud, China Mobile, China Telecom, M-Science, DOCOMO, Ericsson, World Bank

.

[8] La Corea del sud è l'unica area geografica tra quelle considerate ha diffondere dati ufficiali sulle sottoscrizioni di servizi 5G attraverso il Ministero della scienza e l'ICT

2. CYBERSECURITY E 5G

2.1. TRA DISCRIMINAZIONE GEOGRAFICA E *RISK ASSESSMENT*

Il *roll-out* delle reti 5G, che risulta quanto più strategico in considerazione del potenziale spostamento, da parte di molteplici settori industriali, di una quota crescente delle proprie attività su reti di nuova generazione, sta avvenendo in un contesto in cui la c.d. "minaccia cibernetica" mostra una relativa stabilizzazione.

I dati forniti dal Clusit sull'evoluzione degli **attacchi informatici** negli ultimi sei anni, sebbene complessivamente in crescita (nel 2019 +7,6% sul 2018), in particolare per via del *Cybercrime* (i crimini informatici), presentano una sensibile diminuzione per quanto concerne la *Cyber Warfare*, l'insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico[9]. Questi ultimi, infatti, appaiono in sensibile riduzione almeno in termini numerici, passati da 56 del 2018 a 35 nel 2019 (-37,5%).

TABELLA 2.1 Tipologia di attacchi

Attaccanti per Tipologia	2014	2015	2016	2017	2018	2019	2019/2018	Trend
Cybercrime	526	684	751	857	1232	1383	12.3%	↑
Hacktivism	236	209	161	79	61	48	-21.3%	↓
Espionage/Sabotage	69	96	88	129	203	204	0.5%	→
Cyber Warfare	42	23	50	62	56	35	-37.5%	↓
Espionage/Sabotage + Cyber Warfare	111	119	138	191	259	239	-7.7%	→
TOTALE	**873**	**1012**	**1050**	**1127**	**1552**	**1670**	**7,60%**	→

Fonte: Rapporto Clusit 2020

A tal proposito, anche la relazione sulla politica dell'informazione per la sicurezza 2019[10], pur non fornendo i dati in termini assoluti per ragioni di riservatezza, indica come le manifestazioni "critiche" del fenomeno evidenzino un **numero complessivo di azioni "ostili" quasi dimezzato** rispetto al 2018, dopo il picco registrato tra il 2017 e il 2018. In termini percentuali, i dati forniti confermano, tra i target privilegiati, le amministrazioni pubbliche (72% nel 2018 e 73% nel 2019) e

[9] Rapporto Clusit 2020 sulla sicurezza ICT in Italia, pag. 217.
[10] Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza
2019", febbraio 2020

in particolare Ministeri (34% nel 2019, a fronte del 24% del 2018), mentre scende la quota di enti locali attaccati (regionali, provinciali e comunali, che compongono il 16%), a scapito di enti pubblici di altra natura (in quali raggiungono quota 50%). Tra i privati, i soggetti più colpiti fanno capo al settore energetico (che nel 2019 ha subito il 13% degli attacchi complessivi, in crescita dall'11% nel 2018), alle infrastrutture digitali (dal 3% del 2018 al 10% del 2019), alle telecomunicazioni (7% nel 2019), e al settore bancario (anch'esso al 7%).

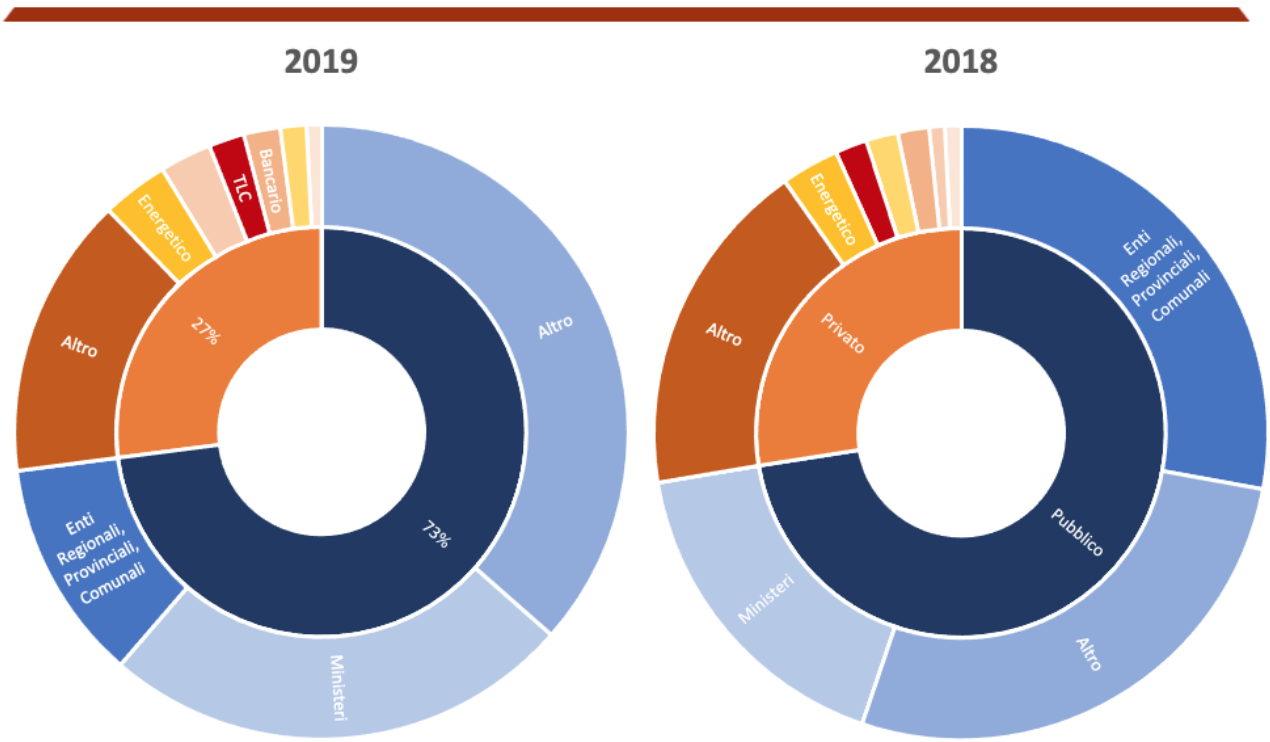

FIGURA 2.1 Attacchi per tipologia di target
Fonte: Relazione sulla politica dell'informazione per la sicurezza 2019 – Presidenza del Consiglio dei Ministri

A livello di attori (Fig.2.2), gran parte degli attacchi risulta condotto da formazioni hacktiviste (73%), mentre le campagne di matrice statuale risultano in diminuzione (dal 20% del 2018 al 12% del 2019). Tuttavia, la crescente quota di attacchi provenienti da soggetti non identificati potrebbe celare delle accresciute capacità di offuscamento da parte degli attori statuali. Proprio quest'ultimo punto ha alimentato, nel corso degli ultimi due anni, il dibattito relativo alla sicurezza nazionale, in particolare concernente la sicurezza delle informazioni e l'utilizzo, nella realizzazione delle reti 5G,

di componentistica proveniente dagli operatori extra europei ed in particolare cinesi. Tale input, partito dall'Amministrazione americana e indirizzato inizialmente alla *Five Eyes*, l'alleanza di intelligence composta da Usa, Gran Bretagna, Canada, Nuova Zelanda e Australia, allo stato attuale è stato recepito da quest'ultima, in parte dalla Nuova Zelanda[11] e recentemente, dopo un lungo iter, anche dal Regno Unito. Lo stesso invito è stato allargato agli altri Paesi europei, con un'adesione che al momento appare incerta (cfr. capitolo 3.2).

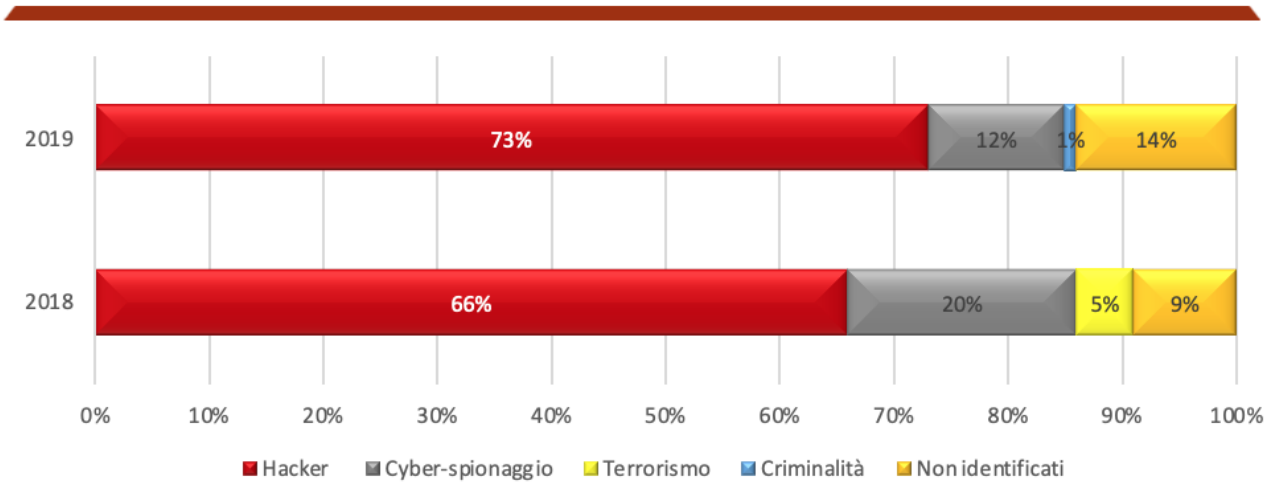

FIGURA 2.2 Attacchi per tipologia di attori
Fonte: Relazione sulla politica dell'informazione per la sicurezza 2019 – Presidenza del Consiglio dei Ministri

In **Italia**, preoccupazioni circa le attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G di provenienza cinese sono state espresse dal Copasir, il Comitato parlamentare per la sicurezza della Repubblica[12]. Quest'ultimo, oltre a ritenere necessario un **innalzamento degli standard di sicurezza** per accedere alla implementazione di tali infrastrutture, rileva che si dovrebbe valutare anche l'ipotesi, ove necessario per tutelare la sicurezza nazionale, di escludere le aziende cinesi dalla attività di fornitura di tecnologia per le reti 5G[13]. Allo stesso

[11] La Nuova Zelanda ha bloccato l'accordo tra un operatore locale ed un vendor cinese.
[12] Copasir, "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", dicembre 2019.
[13] In particolare, le preoccupazioni evidenziate dal Copasir sono relative alla possibilità, per gli organi dello Stato cinese e per le stesse strutture di intelligence del paese del Dragone, di fare affidamento sulla collaborazione di cittadini e imprese sulla base di specifiche disposizioni legislative, come la National Security Law. Quest'ultima obbligherebbe, in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità di pubblica sicurezza militari e alle

tempo, è importante evidenziare come la stessa relazione del Copasir sottolinei la difficoltà di prevedere interventi autoritativi che possano mettere a rischio la realizzabilità di progetti ritenuti essenziali per lo sviluppo delle nuove tecnologie "*in una realtà caratterizzata dalle leggi del mercato e della libera concorrenza*"[14]. Il documento ricorda infatti come lo stesso Governo americano abbia continuamente procrastinato il blocco della fornitura di apparecchiature tecnologiche da parte di aziende cinesi su territorio statunitense, a seguito delle numerose criticità paventate dalle aziende nazionali in conseguenza del predetto divieto.

Nel dettaglio, negli Usa il blocco era stato approvato a maggio 2019, ma ne è stata procrastinata l'effettiva entrata in vigore diverse volte, fino al 15 agosto 2020 e fino al 15 settembre per le aziende terze[15] .

L'ultimo provvedimento, peraltro, ha creato una situazione paradossale per cui anche diverse aziende americane ne risultano danneggiate e hanno chiesto una deroga, mentre l'amministrazione ha specificato come il ban non includa la possibilità, per le compagnie statunitensi, di lavorare con Huawei sullo standard 5G[16]. Per le stesse ragioni, ha sottolineato il Copasir, né gli organi della UE, né i principali Paesi europei hanno finora adottato provvedimenti di divieto o limitazione ex-ante alle attività degli operatori extra-europei.

---

agenzie di intelligence. Inoltre, con riferimento alla normativa sulle attività informatiche, la Cyber Security Law sembra prevedere che gli operatori di rete debbano fornire supporto agli organi di polizia e alle agenzie di intelligence nella salvaguardia della sicurezza e degli interessi nazionali. Esistono tuttavia pareri discordanti in materia. Ad esempio, l'analisi dello studio legale britannico Clifford Chance ha concluso che la legge cinese non conferisce a Pechino l'autorità di obbligare i fornitori di apparati di telecomunicazioni a installare backdoor o dispositivi di ascolto o ad assumere comportamenti che potrebbero compromettere la sicurezza della rete.

[14] Copasir, "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", dicembre 2019, pag. 18.

[15] Dopo il provvedimento di restrizione, inizialmente emanato dal Governo a maggio 2019, il Dipartimento del Commercio aveva fornito all'operatore cinese Huawei una licenza temporanea di 90 giorni per continuare a commerciare smartphone e apparecchiature di rete con aziende e consumatori americani. La licenza è stata poi estesa da agosto a novembre (ulteriori 90 giorni) di ulteriori 45 giorni (quindi fino a febbraio 2020), e poi ancora di 45 fino al 15 maggio 2020, prima dell'ultima estensione, di 90 giorni, che fissano la data di termine della licenza temporanea al 15 agosto 2020. È stato introdotto un ulteriore elemento, estendendo il blocco del trading con Huawei anche a compagnie terze che utilizzano tecnologie americane, come la tailandese TSMC. Nel dettaglio, qualsiasi produttore estero che fornisce chip a Huawei utilizzando strumenti di progettazione, componenti o macchinari statunitensi, dovrà chiedere una licenza *ad hoc* da parte del Dipartimento del commercio. Per tale motivo, al momento della scrittura del presente report, risulta a rischio la produzione di smartphone Huawei con chipset Kirin, e Qualcomm ha chiesto al Dipartimento la licenza per poter fungere da fornitore.

[16] Reuters, U.S. companies can work with Huawei on 5G, other standards: Commerce Department, 15 giugno 2020.

A livello italiano, in particolare, una eventuale discriminazione per nazionalità sarebbe resa complicata anche dall'**alto grado di internazionalizzazione che si riscontra anche tra i network providers, in gran parte a capitale estero** (Fig. 2.3).

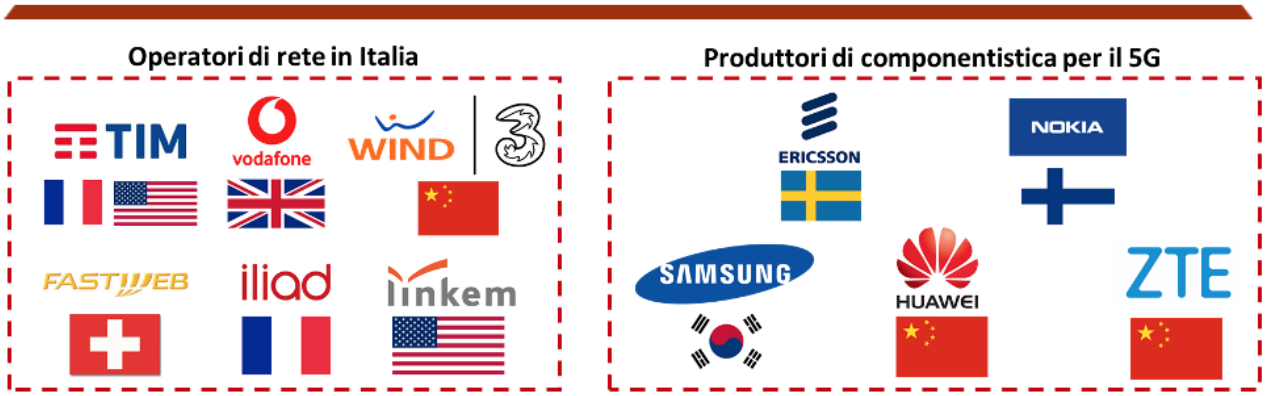

FIGURA 2.3 Nazionalità degli operatori di rete in Italia e dei vendor 5G nel mondo

Fonte: Elaborazioni I-Com

Nel dettaglio, nel mercato italiano sono presenti americani e francesi tra i principali azionisti dell'ex *incumbent* Tim (al momento al centro della possibile transizione verso la rete unica), ancora americani in Linkem, francesi in Iliad, britannici in Vodafone, cinesi in Wind Tre e svizzeri in Fastweb.

Inoltre, per quanto concerne specificamente la **componentistica per il 5G, si osserva come** il **perimetro relativo alle imprese che producono tali apparecchiature sia piuttosto ristretto**, comprendendo prevalentemente Ericsson (Svezia), Nokia (Finlandia), Huawei (Cina), Samsung (Corea del Sud) e ZTE (Cina), che insieme compongono circa il 75% del mercato della fornitura di apparecchiature di rete. Tale concentrazione rende quindi piuttosto complicato attuare una discriminazione per nazionalità di provenienza dei fornitori, a fronte della previsione di misure specifiche per mitigare i rischi a 360 gradi. A tal proposito, si osserva come il Governo italiano abbia assunto una posizione sostanzialmente allineata a quella dei principali partner europei, che hanno scelto di rafforzare le misure di sicurezza e di vigilanza senza imporre esclusioni o limitazioni all'ingresso di soggetti extraeuropei nello sviluppo e nella fornitura di prodotti e servizi relativi alle reti 5G (cfr. cap.3.2).

In Italia, il Presidente del Consiglio ha sottolineato come "*decisioni che limitino la presenza di tali aziende [vendor 5G] dal mercato nazionale non sarebbero coerenti con i principi economici e*

commerciali praticati nel nostro Paese e nel mondo occidentale"[17]. Per tali ragioni, si è puntato sul *risk assessment* e sul rafforzamento del potere di controllo sia normativo (tramite estensione del golden power, cfr. Cap. 4) che *on field*, con la costituzione del CVCN, l'istituzione perimetro di sicurezza nazionale cibernetica (un'area di protezione rafforzata degli asset ICT strategici in sinergia interistituzionale e pubblico - privato) e la costituzione del Computer Security Incident Response Team-CSIRT italiano (presso il DIS, si affianca al punto di contatto unico NIS e al Nucleo per la Sicurezza Cibernetica-NSC, anch'essi istituiti presso il Dipartimento). Il *risk assessment* è stato elaborato dal Comparto intelligence, di concerto con il MiSE, con l'Agcom e con il supporto degli operatori assegnatari di frequenze. Utilizzando un approccio basato su parametri oggettivi (cioè in base alle caratteristiche della nuova tecnologia), le operazioni sono state volte in primo luogo ad identificare gli asset più rilevanti dell'architettura 5G, e poi ad analizzarli in relazione ai profili di rischio rispetto a intenzioni, mezzi e capacità degli attori ostili[18].

Come mostrato in Fig.2.4, è stata definita una mappa del rischio per i componenti dell'architettura 5G in relazione al livello di intensità e alla probabilità. Le azioni identificate sono di 3 tipi: mitigazione nel caso di funzioni cruciali o molto probabilmente attaccate; mitigazione/trasferimento/aggiramento nel caso di funzioni mediamente cruciali o mediamente a rischio; mitigazione/aggiramento/accettazione nel caso di minacce poco probabili o apportate a funzioni non cruciali. Nel dettaglio, in questo ultimo segmento vengono collocate le minacce relativi all'intercettazione di flussi di dati da parte delle Autorità, identificate con una bassa probabilità e un medio livello di rischio. Più probabili ma meno rischiose vengono considerate le minacce al *Network Access Security Management*, nello specifico il traffico di segnalazione (*control plane*) per l'autenticazione e controllo accessi. Di media probabili e medio livello di rischio, cui applicare misure di livello 2, sono le funzioni che fanno capo al EUSP flusso dati utente nell'edge computing (*user plane*), USP e UAADCN (i dati del profilo utente nei terminali e nella rete centrale), C-RAN (tecnologie di accesso radio di nuova generazione). Presentano un'alta probabilità di essere attaccate, anche se con effetti di medio rischio, le funzioni della rete centrale (slicing della rete e SBAAPI, interfacce di gestione dei servizi basati su applicazioni). La parte più delicata della rete, che presenta un rischio di attacco giudicato medio, è costituita dai sistemi di gestione e orchestrazione

[17] Copasir, "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", dicembre 2019, pag. 19.

[18] Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza
2019", febbraio 2020

delle risorse. Anche il DPCM del 7 agosto 2020 va nella direzione del *risk assessment* effettivo, rafforzando il coinvolgimento degli operatori di rete nelle operazioni di verifica delle forniture delle apparecchiature di rete[19].

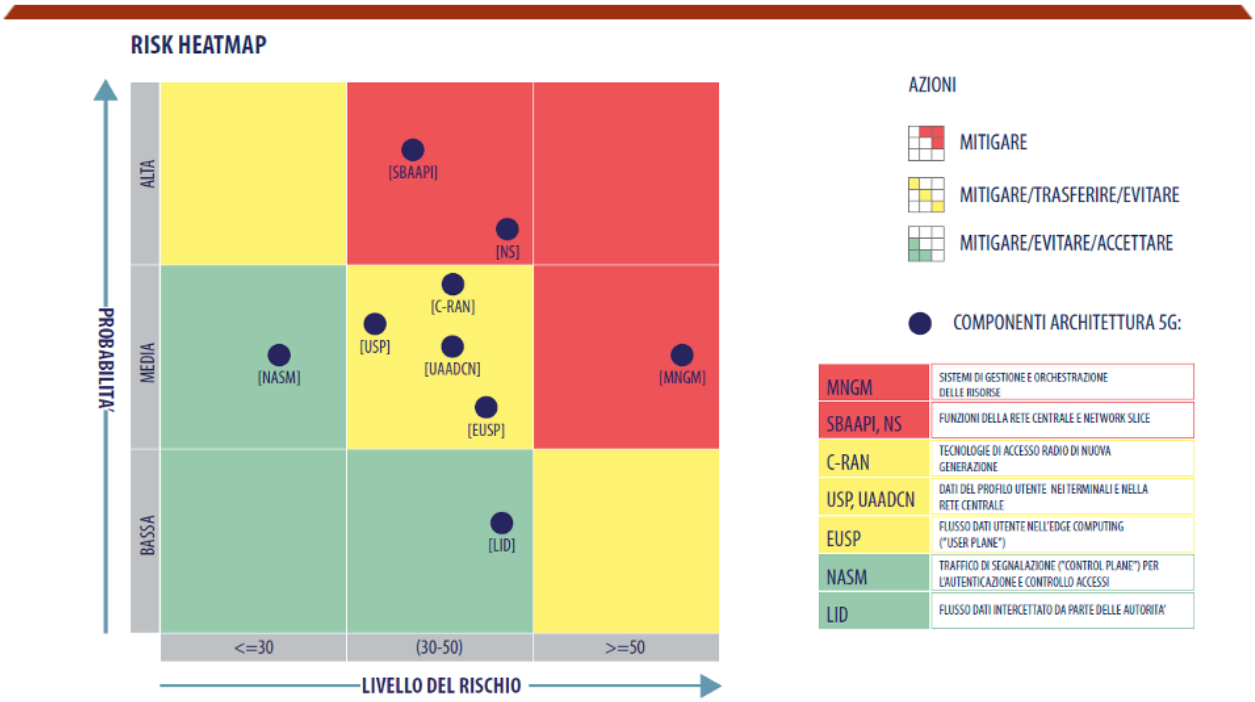

FIGURA 2.4 *Risk assessment* nazionale sul 5G

Fonte: Sistema di Informazione per la Sicurezza nella Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2019", febbraio 2020

2.2. STRUTTURA DELLE RETI, MINACCE E MISURE PER AUMENTARE LA SICUREZZA

La querelle relativa alla sicurezza nazionale e all'opportunità di utilizzare apparecchiature di rete fornite da operatori provenienti da Paesi esterni al blocco atlantico si basa anche su un'importante questione di fondo: la natura composita delle architetture 5G determina l'**impossibilità di realizzare reti ICT che siano al 100% sicure**. Appaiono inefficaci, infatti, i sistemi di sicurezza IT tradizionali, come ad esempio i "*Common Standard Criteria*", poiché le future reti 5G saranno

[19] Nel DPCM del 7 agosto 2020, in ordine alla notifica della società TIM S.p.a. avente ad oggetto la stipula di quattro contratti con Huawei Technologies Italia S.r.l., vengono dettagliate una serie di prescrizioni in capo all'ex-incumbent TIM per la verifica delle apparecchiature fornite dall'operatore cinese Huawei.

costituite da sistemi interconnessi e dotati di software aggiornati di frequente. Altre operazioni quali il *security assessment*, le revisioni del codice e i *penetration test* possono migliorare la qualità del software ma non possono garantire l'assenza di codici malevoli o *backdoor*. Ciò è dovuto al fatto che tali sistemi sono composti da miliardi di transistor e milioni di righe di codice, realizzati in forma modulare. Inoltre, a seconda della propria dimensione, i produttori sviluppano in-house dal 10% al 30% della componentistica hardware e software, mentre il resto viene approvvigionato in outsourcing attraverso la supply chain. Tale interdipendenza determina una condizione in cui la sicurezza dipende da tutti gli attori della catena e non da uno soltanto.

Il National Institute of Standards and Technology (Nist) definisce il processo di identificazione e mitigazione dei rischi associati alla natura distribuita e interconnessa delle supply chain di prodotti e servizi IT (e OT) come *Cyber Supply Chain Risk Management* (C-SCRM). Poiché le minacce e le vulnerabilità della supply chain potrebbero compromettere prodotti e servizi in ogni fase del ciclo, sia intenzionalmente sia involontariamente, in questo processo è incluso l'intero ciclo del sistema, ovvero design, sviluppo, distribuzione implementazione, acquisizione, manutenzione e distruzione.

Secondo il Nist, i rischi sono associati prevalentemente alla mancanza di visibilità (*visibility*), di *understanding* e/o di controllo di molti dei processi e delle decisioni coinvolte tanto nello sviluppo quanto nell'acquisizione e nella fornitura di prodotti e servizi IT. L'Istituto propone una tassonomia che distingue le minacce e le vulnerabilità tra conflittuali (cioè derivanti da attacchi), e non

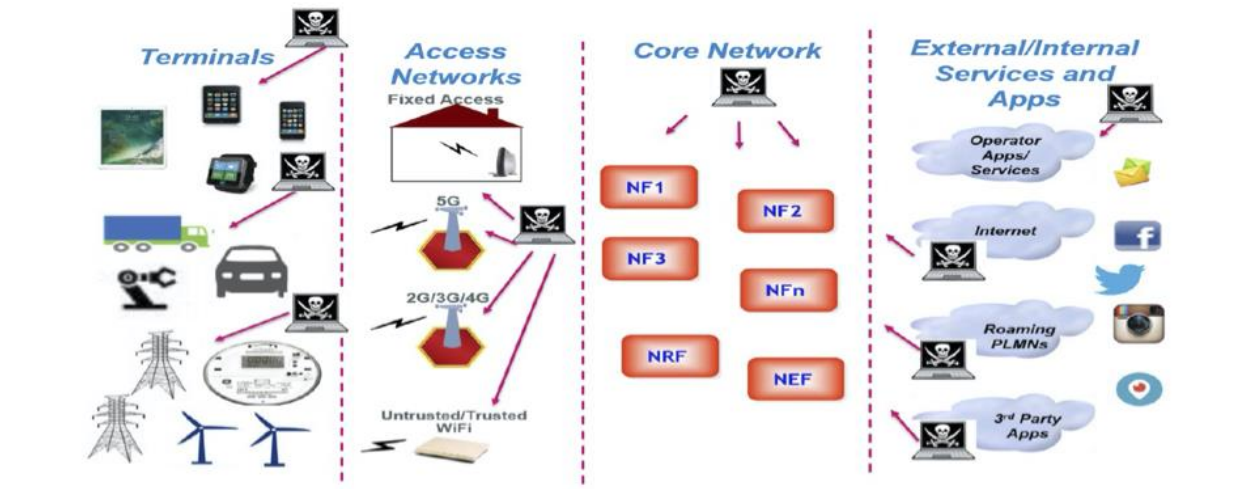

FIGURA 2.5 The 5G Threat Landscape

Fonte: 5G Americas, "The Evolution of Security in 5G. A Slice of Mobile Threats", luglio 2019

conflittuali (dovute a scarsa qualità o disastri naturali), sia interne (relative alle procedure organizzative) che esterne (collegate alla supply chain in cui opera l'azienda o l'organizzazione). Per i sistemi critici, una mitigazione dei rischi efficace richiede agenzie deputate all'identificazione di sistemi e componenti che sono più vulnerabili e che possano avere il maggiore impatto se compromesse.

Per quanto concerne le reti 5G, l'estensione delle reti a nuovi ambiti e applicazioni determina una crescente complessità e interconnessione, insieme ad un allargamento delle superficie su cui possibili malintenzionati possono sferrare i propri attacchi. Tale allargamento dipende in buona sostanza da quello che viene definito il *Massive IoT*, ovvero la diffusione di sensori, device e apparecchiature capaci di comunicare tramite protocolli di rete (IP) e talvolta di agire nel mondo fisico.

Nel dettaglio, la sicurezza della rete 5G dovrà essere garantita su 4 diversi domini: i terminali, la rete di accesso, la rete core e le applicazioni e i servizi di terze parti. I **terminali** costituiscono il primo target per via della immensa di diffusione di smartphone, per le molteplici modalità di connessione disponibili e per altri fattori di vulnerabilità. Gli attacchi ai terminali possono essere classificati in 4 categorie: *Mobile to Infrastructure* (schema in cui molti device infetti attaccano l'infrastruttura per metterla fuori gioco); *Mobile to Internet* (molti device infetti attaccano siti pubblici per renderli indisponibili); *Mobile to Mobile* (molti device infettano altri device e/o causano disservizi); *Internet to Mobile* (codici malevoli diffusi sul web tramite app, giochi o video per infettare i terminali). Il secondo ambito è costituito dalla **rete di accesso** che, passando al 5G, erediterà tutte le sfide relative alla sicurezza delle reti precedenti (2G, 3G, 4G e Wi-Fi). Gli attacchi che vengono condotti su questa parte della rete (Fig. 2.5) mettono a rischio prevalentemente la privacy dell'utente, mentre i rischi per le funzionalità strutturali sono più limitati.

Uno degli attacchi più comuni al network access è costituito dalla *Rogue Base Station* (RBS) threat: una stazione "pirata" si camuffa da stazione autorizzata per creare un attacco "*Man in the Middle*", in cui i malintenzionati si pongono a mezza via tra le rete e i terminale dell'utente, intercettandone quindi le comunicazioni, tracciandone gli spostamenti e avendo la possibilità di manomettere le informazioni trasmesse e causare potenziali attacchi di tipo DoS (*Denial-of-Service*) a servizi e applicazioni (che comportano la richiesta dello stesso servizio da parte di molteplici terminali allo stesso tempo per farne venire meno le funzionalità o i servizi interi). Questo tipo di minaccia esiste dalla nascita delle reti GSM e probabilmente continuerà ad esistere ed evolversi con l'evoluzione

delle reti mobili. A tal proposito, si osserva come le reti 5G abbiano dei dispositivi di sicurezza più avanzati rispetto a quelli del 4G, ma anche con lo standard 5G sono possibili una serie di attacchi tramite RBS, ad esempio sfruttando la fase di transizione dalla rete LTE alla rete 5G per attaccarne i punti più deboli e causare malfunzionamenti e disservizi. Il terzo dominio è costituito dalla **rete core**, la parte che gestisce le funzioni di rete più importanti, ovvero *l'Access and Mobility Management Function* (AMF), *l'Authentication Server Function* (AUSF) e *lo Unified Data Management* (UDM). L'AUSF conserva i dati per l'autenticazione degli apparecchi utente (UE), mentre l'UDM immagazzina i dati di registrazione. Poiché queste sono funzioni critiche nelle reti 5G, un attacco DDoS (*Distributed Denial-of-Service*) contro di loro, sia che avvenga da internet o da una *botnet* mobile, potrebbe potenzialmente ridurre significativamente la disponibilità di servizi 5G o persino causarne l'interruzione. Di conseguenza, la parte core della rete si configura come la sezione più importante da proteggere, in particolare se si vuole garantire la continuità di funzionamento della maggior parte dei servizi e delle applicazioni che transitano su di essa, soprattutto di quelli critici. Per tali ragioni, le norme approvate in alcuni Paesi europei prevedono tutele speciali per questa parte della rete, o diversificazioni finalizzate a ridurre il rischio di una compromissione totale della rete. Il quarto dominio è costituito da **Applicazioni e servizi di terze parti** (prevalentemente OTT) ospitati dagli operatori. In questo contesto il livello di sicurezza dipende dalla qualità delle applicazioni esterne, dall'*expertise* dei loro sviluppatori e dalle operazioni di aggiornamento e manutenzione. In questo caso, infatti, uno dei rischi potrebbe essere costituito dalla minore esperienza in cybersecurity da parte degli sviluppatori di tali servizi terzi.

Tra i fattori che determinano l'allargamento del perimetro di attacco si evidenzia anche il c.d. *edge computing*, ovvero la distribuzione di piccoli data center dotati di capacità di elaborazioni che siano il più possibile vicini all'"*edge*" (cioè al "limite" o al "margine" della rete) che devono servire al fine di garantire la latenza *ultra low* necessaria per i servizi avanzati di IoT. Inoltre la tecnologia del *network slicing*, che consente ad una molteplicità di reti logiche di agire indipendentemente su una comune rete fisica, aumenta ancor di più i potenziali rischi, poiché possibili intrusioni che avvengono tramite un comparto potrebbero estendersi anche agli altri. Per tali ragioni, sono necessarie specifiche misure, ad esempio l'isolamento delle risorse e quello delle "*slice*", in modo da bloccare richieste di risorse eccessive da parte di singoli layer e di impedire che tramite una "fetta" sia possibile accedere e modificare le informazioni contenute in un'altra "fetta" della rete.

Le principali misure di sicurezza contenute nelle architetture di rete 5G sono evidenziate nella fig. 2.6 (Fonte: Enisa). Una premessa importante per comprendere la complessità della gestione della

sicurezza nelle reti 5G è relativa alla distinzione tra attacchi *zero days* e attacchi *day-one*: mentre con i secondi si identificano gli attacchi per i quali esiste già uno storico e un'"impronta", con *zero days* vengono indicate le minacce che non sono ancora state attuate. Di conseguenza, se per gli attacchi *day-one* esistono già strategie per prevenirli e contrastarli, i controlli di sicurezza per gli zero days consistono prevalentemente nell'identificazione di deviazioni rispetto ai comportamenti già noti e considerati "corretti" da parte dei carrier cloud e delle applicazioni, mentre le azioni difensive consistono nella mitigazione degli attacchi e nell'ottenimento del maggior numero di informazioni relative alle minacce, in modo da identificarle e contrastarle nel modo più appropriato.

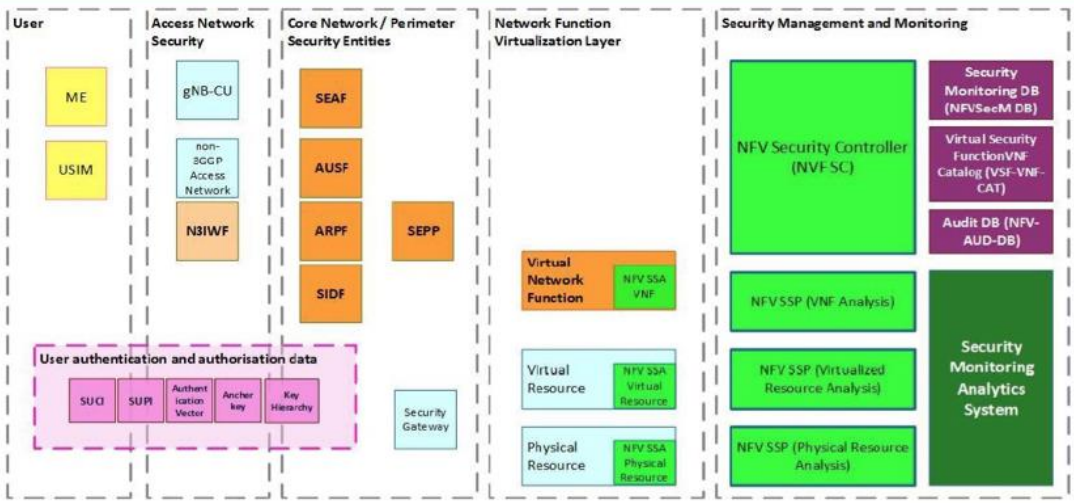

FIGURA 2.6 Security Architecture zoom-in

Fonte: ENISA Threat Landscape For 5G Networks, novembre 2019

La mitigazione delle minacce si basa sulla vasta mole di dati di cui gli operatori di rete mobile dispongono, relativi alle applicazioni che essi rendono disponibili sulle proprie reti. Sulla base di queste informazioni gli operatori creano schemi di processi iterativi (cioè che si ripetono) e monitorano le correlazioni di vari elementi (ad esempio le coordinate di geolocalizzazione e gli *analytics* relativi ai comportamenti delle applicazioni) per confrontarli con gli schemi rilevati in caso di minacce. In tal modo, specifici sistemi si occupano di identificare queste ultime nel modo più accurato possibile e di innescare, in caso di bisogno, le opportune procedure di sicurezza in modo automatico.

La mappa degli elementi di sicurezza delle reti 5G è piuttosto complessa. Quella elaborata da Enisa suddivide il perimetro in 5 aree: *User*, *Access Network Security, Core Network Security Entities, Network Function Virtualization Layer e Security Management and Monitoring.* Nel lato *User* si trovano tutti i device che possono interagire con la rete 5G, definiti *Mobile Equipment* (ME) ovvero sensori, componenti di sistemi IoT, rilevatori *e-Health* etc, cui viene garantito l'accesso tramite modulo identificativo USIM[20] e *Internet Key Exchange*[21]. Per l'autenticazione alla rete di accesso e alla rete core vengono utilizzati specifici identificatori 5G indipendenti dai singoli device, sia permanenti che temporanei[22].

Nel perimetro della rete core si trovano diverse funzioni di sicurezza, tra cui:

- la *Security Anchor Function* (SEAF), che si occupa di generare una chiave di ancoraggio unificata per l'autenticazione primaria, che può essere utilizzata dal device e dalla rete di servizio per proteggere le comunicazioni successive;
- l'*Authentication server function* (AUSF) che deve gestire le richieste di autenticazione[23];
- *l'Authentication credential Repository and Processing Function* (ARPF), che ha la funzione di selezionare un metodo di autenticazione basato sull'identità dell'utente e sulla policy di gestione, e di elaborare i dati di autenticazione e i materiali di codifica[24].

---

[20] Lo *Universal Subscriber Identity Module* (USIM, l'equivalente della SIM card nel 5G) che consiste nel modulo identificativo utilizzato nell'accesso e nelle comunicazioni nelle reti 5G indicato nelle specifiche del 3GPP.

[21] La sicurezza per l'accesso non 3GPP alla rete 5G Core è ottenuta mediante una procedura che utilizza Internet Key Exchange, protocollo usato per implementare le associazioni di sicurezza nell'IP, come definito nella RFC 7296 per impostare una o più associazioni di sicurezza ESP IPsec. Il ruolo di iniziatore (o client) IKE è assunto dall'User Equipment e il ruolo del responder IKE (o server) è assunto dal Non-3GPP Interworking (N3IW).

[22] Tra gli identificatori del 5G si annoverano il *Subscription Permanent Identifier* (SUPI) e il *Subscription Concealed Identifier* (SUCI). A ciascun utente nel sistema 5G è assegnato un SUPI, ovvero un identificatore permanente di sottoscrizione 5G, da utilizzare all'interno del sistema 3GPP. Il SUCI, invece, è un identificatore nascosto che preserva la privacy dell'utente e contiene il SUPI nascosto. Infatti, il sistema 5G supporta l'identificazione degli utenti indipendentemente dall'identificazione dei device. Per ogni device l'accesso al sistema 5G deve avere un identificatore di apparecchiatura permanente (PEI). Il sistema 5G supporta l'assegnazione di un identificatore temporaneo (5G-GUTI) al fine di consentire la protezione della riservatezza degli utenti.

[23] Le richieste di autenticazione possono avvenire sia per l'accesso 3GPP sia per l'accesso non 3GPP (non verificato). L'AUSF fornisce il SUPI (l'identificativa permanente) alla rete dell'operatore mobile visitata (Visited Public Land Mobile Networks o VPLMN), solo dopo la conferma dell'autenticazione se la VPLMN ha inviato una richiesta di autenticazione con SUCI.

[24] A queste si aggiungono la SIDF e la SEPP. La *Subscription Identifier De-concealing Function* (SIDF) è incaricata di rimuovere l'occultamento dell'identificatore nascosto (SUCI). Il *Security Edge Protection Proxy* (SEPP), introdotto nell'architettura 5G come entità situata sul perimetro della rete mobile, funge da nodo proxy non trasparente. Si

Per quanto concerne il quarto dominio, è importante osservare come la *Network Function Virtualisation* (NFV) introduca un nuovo concetto per i fornitori di servizi, che consiste nell'uso delle tecnologie di virtualizzazione IT standard applicate alla distribuzione delle funzioni di rete con l'obiettivo di fornire più rapidamente nuovi servizi di rete. Nel dettaglio, una VNF consiste in una virtualizzazione di una funzione di rete in una rete *legacy* non virtualizzata[25]. Lo scopo delle funzioni di sicurezza è dunque garantire che queste funzioni virtualizzate, anche molto diverse tra loro, operino in maniera sicura, e che un eventuale minaccia verso una di esse non si propaghi alle altre. A livello tecnico, gli elementi di sicurezza nel dominio della virtualizzazione delle funzioni di rete sono costituiti da:

- una serie di *NFV Security Services Agent* (SSA NFV), ovvero uno per ogni funzione virtualizzata, responsabili della ricezione sicura delle policy di monitoraggio della sicurezza (*Security Monitoring policy*) e dell'attuazione delle stesse[26];
- un *NFV Security Controller* (SC) che si occupa dell'orchestrazione delle politiche di sicurezza del sistema svolgendo molteplici funzioni di certificazione, tra cui gestire i *Security Services Agent* delle diverse funzioni di rete virtualizzate per mantenerli in uno stato coerente in base alla policy specificata[27];
- un *NFV Security Services Provider* (NFV SSP), responsabile dell'orchestrazione della politica di monitoraggio della sicurezza ricevuta dal *Security Controller* (NFV SC). Quest'ultimo, in particolare, interagisce con vari componenti per implementare le policy attraverso diversi sistemi, che comprendono sia le infrastrutture di virtualizzazione delle funzioni di rete, sia

occupa di filtrare e controllare i messaggi sulle interfacce del piano di controllo tra reti degli operatori mobili e di nascondere la topologia (ovvero la struttura geometrica) della rete.

[25] ETSI GS NFV 001 fornisce un elenco di casi d'uso ed esempi di funzioni di rete di destinazione (NF) per la virtualizzazione https://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[26] Esso opera sia nel dominio delle infrastrutture di virtualizzazione delle funzioni di rete (*Network Function Virtualisation Infrastructure*, NFVI, che nel dominio delle funzioni di virtualizzazione della rete (*Virtual Network Function*).

[27] Il *NFV Security Controller* assicura anche l'accoppiamento tra il *Virtual Network Function Manager* (VNFM) e gli *Element Management* degli SSA, ne permette la personalizzazione, ne gestisce le credenziali, facilita il clustering di più SSA in un'apparecchiatura distribuita e li monitora rispetto a guasti e rimedi. *VNF Manager* è responsabile della gestione del ciclo di vita di VNF (ad es. iniziazione, aggiornamento, query, ridimensionamento e terminazione). Ciascuna delle slice che servono un tenant comprende uno o più VNFM. L'*Element Management* è responsabile della configurazione per le funzioni di rete fornite da VNF, della gestione dei guasti per le funzioni di rete fornite dal VNF, della raccolta dei risultati della misurazione delle prestazioni delle funzioni fornite dal VNF e della gestione della sicurezza delle stesse funzioni VNF.

le funzioni di virtualizzazione della rete, ed è responsabile della ricezione dei dati di telemetria da vari *Security Service Agents* (SSA);

- un *Security Monitoring Analytics System*, che si occupa di ricevere in modo sicuro la telemetria del *Security Monitoring* da tutto il sistema di *Network Function Virtualisation* (NFV), incluse tutte le infrastrutture di virtualizzazione delle funzioni di rete (*Network Function Virtualization Infrastructure*), anche geograficamente distribuite. Il *Security Monitoring System* applica tecniche avanzate di *machine learning* sulla telemetria per eseguire il rilevamento di anomalie di sicurezza e minacce emergenti nel sistema, anche sulla base di database continuamente aggiornati che includono molteplici parametri di sicurezza[28]. Può anche attivare azioni correttive tramite Security Controller NFV.

Ricapitolando, i principali miglioramenti della sicurezza in 5G, definiti dal 3GPP, includono:

- comunicazioni sicure e meccanismi avanzati di crittografia e protezione dell'integrità finalizzati a proteggere lo *user plane*, il control plane e la gestione del traffico;
- un framework di autenticazione unificato per le varie tecnologie e dispositivi di accesso;
- la protezione della privacy degli utenti in relazione alle informazioni che possono essere utilizzate entità non autorizzate per identificare e tenere traccia degli utenti (ad esempio, proteggendo identificatori permanenti come SUPI, IMSI e IMEI);
- un sistema avanzato di protezione degli User Equipment dagli attacchi tramite *Rogue Base Station*;
- un'architettura di sicurezza basata sui servizi che consente l'isolamento delle sezioni per prevenire la diffusione di attacchi ad altre slices della rete.

Nel complesso, due fattori diventeranno sempre più critici nelle evoluzioni future: velocità e automazione. Se è verosimile che la velocità di identificazione delle nuove minacce verrà progressivamente migliorata, la creazione di difese automatizzate per garantire la più rapida

[28] Il *Security Monitoring Database*[28] include criteri e configurazioni di monitoraggio della sicurezza, credenziali di sicurezza per agevolare le comunicazioni sicure tra i vari componenti di Security Monitoring e credenziali per l'archiviazione sicura dei dati di telemetria, incluse policy di sicurezza di specifici tenant. Il NFV *Security Monitoring Database* (NFV SecM-DB) contiene dati utilizzati per sviluppare il monitoraggio della sicurezza a livello di sistema NFV (Network Function Virtualisation). Il *SA/VSF Catalog Database* (VSF-NVNF-CAT) è un archivio per i *Security Services Agents* come le funzioni di sicurezza virtuale (VSF) delle funzioni di rete virtuale (Virtual Network Function). Il catalogo ha la capacità di aggiungere e rimuovere pacchetti e / o immagini dei *Security Services Agents* e include anche un VNFD (*Virtual Network Function Descriptor*) contenente metadati e informazioni su quella specifica funzione virtuale di sicurezza (VSF) della funzione della rete virtuale (VNF). L'*Audit DB* (NFV AUD-DB) è un database sicuro che contiene informazioni per l'audit della sicurezza.

risposta possibile in caso di attacco potrebbe diventare addirittura indispensabile. Infine, poiché il 5G incorporerà progressivamente servizi che riguardano direttamente la vita e il benessere dei cittadini, come la sanità e l'automotive, la sicurezza delle sue reti travalicherà il valore economico, pertanto le sue metriche trascenderanno quelle che tradizionalmente fanno capo alla sicurezza dei sistemi IT. Per tali ragioni, la sicurezza di tali reti è divenuta e diverrà sempre più una questione di interesse governativo, e potrà essere complicata dal fatto che molteplici autorità (altre nazioni, enti internazionali) vorranno imporre una serie di requisiti diversificati a diversi livelli e/o in diverse parti del mondo. Pertanto la sicurezza del 5G, in quanto standard globale, rischia di dover sottostare, oltre che ad una lunga serie di funzioni e parametri tecnici, ad un complesso e diversificato ambiente normativo.

2.3. VERSO UNA STANDARDIZZAZIONE INTERNAZIONALE: SECAM, SCAS, NESAS

Per ovviare alla moltiplicazione e diversificazione degli ambienti normativi, una possibile soluzione è costituita dalla **standardizzazione internazionale**. Per le reti mobili, esempi di questo genere sono rintracciabili già nella progettazione della prima rete mobile GSM, che mirava a consentire il roaming e quindi la possibilità per i consumatori europei di poter portare il proprio dispositivo mobile in un altro paese continentale, utilizzare una rete mobile straniera e usufruire dei servizi in loco, fatturati però dal proprio operatore domestico. Per raggiungere questo risultato, tra la fine degli anni '80 e l'inizio degli '90, è stato necessario implementare una collaborazione piuttosto intensa tra le diverse parti interessate, tra cui gli Stati, che si sono accordati per riservare specifiche bande di frequenza a tale utilizzo, e alcuni operatori di rete, che hanno contribuito a sviluppare lo standard, divenuto operativo a partire dal 1992[29]. Il successo del GSM ha poi attratto sempre più operatori di rete anche al di fuori dell'Europa, trasformando la rete operante in GSM nella prima vera rete mobile mondiale.

Anche lo standard successivo, chiamato 3G (a livello tecnico UMTS e WCDMA), è stato progettato attraverso un'iniziativa congiunta, in questo caso con portata globale, ovvero il 3GPP (*3rd Generation Partnership Project*)[30]. Il 3GPP ha progressivamente rilevato le attività di gestione delle

[29] Successivamente, la responsabilità ed il controllo dello standard GSM è stato trasferito all'European Telecommunications Standards Institute (ETSI), ed anche i vendor delle apparecchiature di rete hanno cominciato a partecipare alle attività di standardizzazione.

[30] Fondato nel 1998 e tutt'ora attivo, comprende operatori di rete e vendor di tutto il mondo e si occupa di coordinare i lavori per definire le funzioni e i protocolli delle reti mobili.

specifiche GSM dall'ETSI e, allo stato attuale, tutti gli standard concordati e approvati dal 3GPP sono automaticamente riconosciuti e ratificati dagli organismi di standardizzazione nazionali o internazionali[31]. La partecipazione al 3GPP è aperta ad ogni soggetto dell'industria della telefonia mobile che sia membro di uno degli enti di regolamentazione di Europa, Usa e Giappone, inclusi i vendor di apparecchiature, i produttori di device mobili, gli operatori di rete, le autorità di regolazione e altri tipi di organizzazioni e gruppi di interesse. Di conseguenza, tale vasta adesione fa sì che gli standard emanati dal 3GPP siano generalmente accettati dalla maggioranza degli operatori e dei Paesi. L'ente è organizzato in vari *Technical Specification Groups* (TSG) suddivisi per temi (ad es. funzioni e protocolli di rete, crittografia, autenticazione e sicurezza) e sottogruppi (*Working Groups*). Il gruppo SA3, in particolare, è responsabile per gli aspetti relativi alla sicurezza, ed ha il compito di analizzare ogni nuova caratteristica sviluppata all'interno del 3GPP specificandone i requisiti ed i meccanismi per garantirne la protezione[32].

L'obiettivo finale delle operazioni del 3GPP consiste nell'assicurare una **completa interoperabilità tra le reti dei diversi operatori e nei diversi Paesi,** in modo che potenzialmente tutti i device mobili funzionino su tutti i network. Inoltre, per ogni generazione di standard è presente un numero piuttosto consistente di release delle specifiche tecniche, che vengono implementate nelle apparecchiature di rete dei vendor e nelle infrastrutture degli operatori di reti. Il lavoro sulla sicurezza 5G, in particolare, è iniziato nel 2016 e, nell'estate del 2018, il gruppo SA3 ha consegnato la prima versione di una nuova specifica tecnica per la sicurezza 5G (la specifica numero 33.501), che include le informazioni di base sull'architettura di sicurezza generale e sui meccanismi per i sistemi 5G (ad es. il modo in cui i dispositivi sono autenticati dalla rete, come viene protetta la comunicazione tra il dispositivo e la rete e anche all'interno di una rete 5G tra le diverse funzioni di rete). Parallelamente, un forte impulso verso la standardizzazione è stato dato anche dalla GSM Association[33], nata come associazione di categoria e progressivamente coinvolta nello sviluppo degli standard tecnici.

[31]Attualmente il 3GPP consiste in una partnership mondiale di organismi di standardizzazione per le telecomunicazioni di tutto il mondo e definisce gli standard normativi ufficialmente riconosciuti pressoché in tutti i Paesi del globo. Gli altri organismi sono, oltre allo stesso ETSI in Europa, ATIS (Alliance for Telecommunications Industry Solutions) negli Stati Uniti e TTC (Telecommunication Technology Committee) in Giappone.

[32] Il funzionamento delle procedure è basato su proposte di contributi e meccanismi di approvazione: per far sì che un nuovo principio o una nuova idea vengano implementati in uno standard, questi devono essere portati all'attenzione dei membri per l'approvazione.

[33] La GSM Association è nata durante gli anni del lancio delle reti GSM, in particolare dopo la sottoscrizione di un *Memorandum of Understanding* da parte dei Paesi fondatori, Francia, Germania, Italia e Regno Unito, cui si sono via

Attualmente, ETSI definisce le specifiche tecniche delle funzionalità delle reti mobili, mentre gli aspetti relative ai processi e alle procedure, così come quelli relativi al roaming internazionale, sono in capo a GSMA. Anche quest'ultima è organizzata in vari gruppi di lavoro (WG), ciascuno con un argomento particolare e un'area di competenza, che vanno dagli aspetti tecnici, come la gestione del segnale e la trasmissione e dati tra operatori a livello internazionale, alla gestione internazionale dei registri di fatturazione, fino alla sicurezza e alle frodi, insieme agli aspetti legali relativi a roaming e contrattualistica tra operatori[34]. A livello di sicurezza, l'omologo del SA di 3GPP è costituito dal *Fraud and Security Group* (FASG), che si occupa della sicurezza del segnale radio, delle reti mobili, della configurazione degli apparati di rete, del roaming internazionale e della crittografia, gestendo anche la redazione di specifiche tecniche e linee guida.

Secondo quanto evidenziato dall'ETSI, affinché gli operatori di rete mobile possano valutare il livello di sicurezza raggiunto dai prodotti di rete, tale sicurezza dovrebbe essere misurabile, confrontabile e seguire una base standardizzata comune. A tal fine, il 3GPP ha introdotto la SECAM (Security Assurance Methodology) ed il processo di valutazione ad essa collegato, definendo attività e ruoli dei diversi soggetti coinvolti. Nel dettaglio, la SECAM costituisce un processo usato per misurare le caratteristiche relative alla sicurezza dei prodotti di rete che fanno capo al 3GPP. Il processo di valutazione SECAM comprende l'analisi dei processi con cui i fornitori delle apparecchiature di rete sviluppano i propri prodotti e la valutazione della gestione del loro ciclo di vita. A ciò si aggiunge la creazione di requisiti di sicurezza e specifiche per i test, denominate *Security Assurance Specifications* (SCAS).
Il processo di valutazione SECAM individua anche i diversi compiti di valutazione e gli attori cui questi task vengono assegnati[35]. Tra i vari compiti descritti nello schema SECAM, alcuni sono in capo al 3GPP (che mantiene la responsabilità complessiva sullo schema SECAM e sviluppa le

via aggiunti numerosi altri membri. Registrata formalmente in Svizzera nel 1995, l'Associazione conta attualmente circa 800 membri che operano in oltre 200 Paesi.

[34] Gli WG della GSMA creano specifiche tecniche che non sono formalmente ratificate dagli organismi di standardizzazione riconosciuti, ma sono di fatto vincolanti per gli operatori di rete in quanto soggetti a contratti legali e accordi internazionali di roaming. Di conseguenza, sebbene il meccanismo con cui le specifiche emanate da GSMA vengono adottate è differente, queste sono in sostanza paragonabili agli standard pubblicati dal 3GPP.

[35] Rispetto ai primi si evidenziano l'*assessment* dei processi di sviluppo prodotti dei fornitori delle apparecchiature di rete; la valutazione della gestione del ciclo di vita del prodotto; il *Security Compliance Testing*; il *Basic Vulnerability Testing*; l'*Enhanced Vulnerability Analysis*.

SCASes), mentre altri sono assegnati al c.d. *Accreditation Body*, individuato nella GSMA. La separazione dei compiti tra i due enti è rappresentata anche nella figura 1.

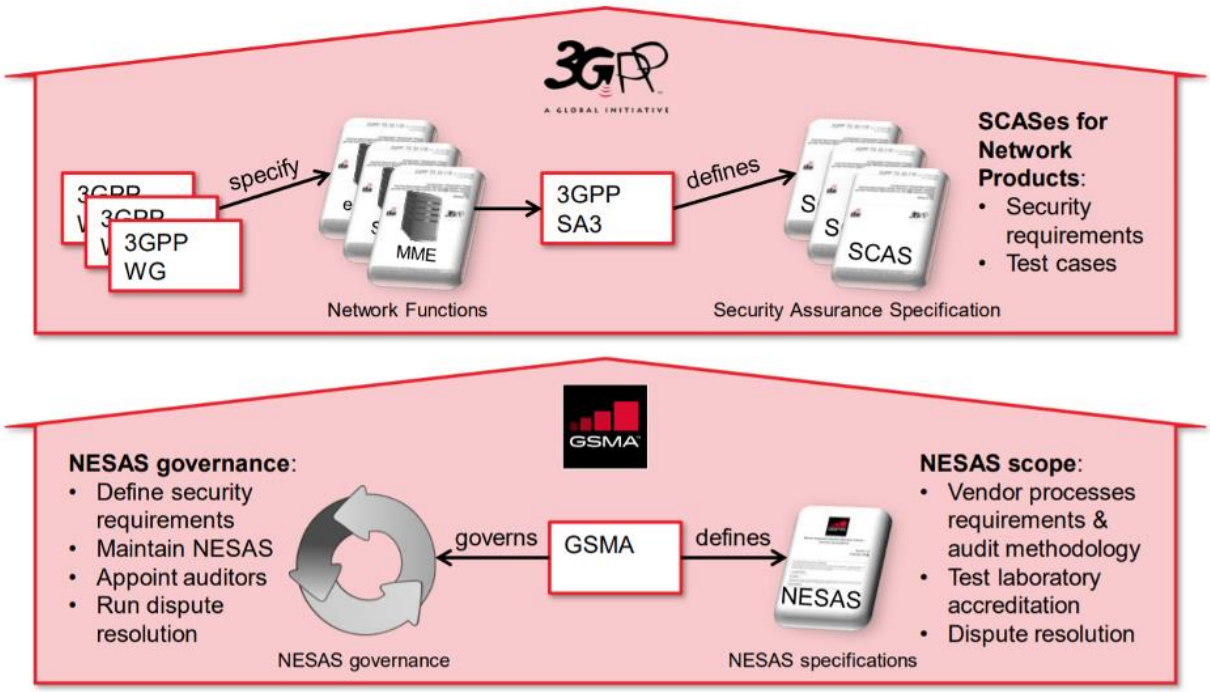

FIGURA 2.7 Ruoli e compiti di 3GPP e GSMA nel SECAM / NESAS

Fonte: GSMA - 2019

A GSMA (parte inferiore della figura), è stato assegnato il compito di:

- definire i requisiti di sicurezza per lo sviluppo dei prodotti di rete da parte dei vendor e per la verifica del processo di gestione del ciclo di vita del prodotto;
- definire la metodologia per l'audit;
- gestire l'accreditamento SECAM per i vendor ed i laboratori indipendenti che effettuano i test[36];

[36] Per garantire l'affidabilità dei risultati della valutazione, è previsto un processo di accreditamento sia dei laboratori di valutazione, sia delle parti rilevanti per la sicurezza dei prodotti di rete e dei processi di gestione del ciclo di vita del prodotto che fanno capo al fornitore. Per i laboratori che effettuano i test, l'accreditamento da parte di un ente esterno serve a verificare le capacità e le competenze necessarie a svolgere i compiti di testing assegnati da GSMA.

- gestire eventuali dispute e reclami;
- definire il proprio schema per coprire tutti questi task.
-

Tale schema, in particolare, è stato definito da GSMA e ribattezzato NESAS, ovvero *Network Equipment Security Assurance Scheme*, e fornisce il framework amministrativo per l'implementazione del SECAM per i controlli di sicurezza delle apparecchiature di rete conformi alle linee guida del 3GPP.
Il NESAS nasce per fornire un insieme comune di **requisiti a garanzia della sicurezza** finalizzati ad introdurre una base comune a tutti i prodotti, indipendentemente dai requisiti individuali del singolo Stato. Tali requisiti e l'intero (e articolato) processo di certificazione, sono pensati per essere utilizzati a livello globale, lasciando che i fornitori di apparecchiature si concentrino sulla creazione e sul miglioramento del prodotto, dovendo garantire la conformità ad un unico insieme di requisiti significativi che al contempo sia in grado di assicurare un efficace livello di sicurezza.

Infatti, la necessità di reti robuste e affidabili tende a spingere i singoli Paesi a muoversi in solitaria nella gestione e certificazione di reti mobili e apparecchiature, rischiando di creare una frammentazione globale che genera criticità per i fornitori di apparecchiature nel rispetto delle molteplici e differenti normative nazionali, produce quindi ritardi e aumentando i costi. Si evidenzia inoltre come la necessità, per i fornitori di apparecchiature di rete, di soddisfare tutti i requisiti nazionali, non migliori necessariamente la sicurezza globale, ma rischi di essere controproducente in caso di requisiti contradditori tra diversi Paesi diversi. Per ovviare a queste controindicazioni, l'obiettivo del NESAS consiste nel mettere insieme un singolo set di requisiti (la c.d. *security baseline)*, che definisce la capacità di un prodotto di resistere agli attacchi. A livello procedurale, la valutazione della sicurezza dello schema NESAS coinvolge diverse fasi e attori (fig. 2.8). Da un lato, si osserva come i test riguardino sia le apparecchiature dei vendor, sia i loro processi interni. Infatti, tutti i vendor hanno processi definiti per lo sviluppo e il ciclo di vita del prodotto e le relative procedure di sicurezza. Una delle valutazioni incluse nella procedura NESAS si basa proprio sul controllo di queste procedure e comprende un insieme combinato di requisiti per i fornitori, che devono dimostrare come raggiungono l'obiettivo della sicurezza.

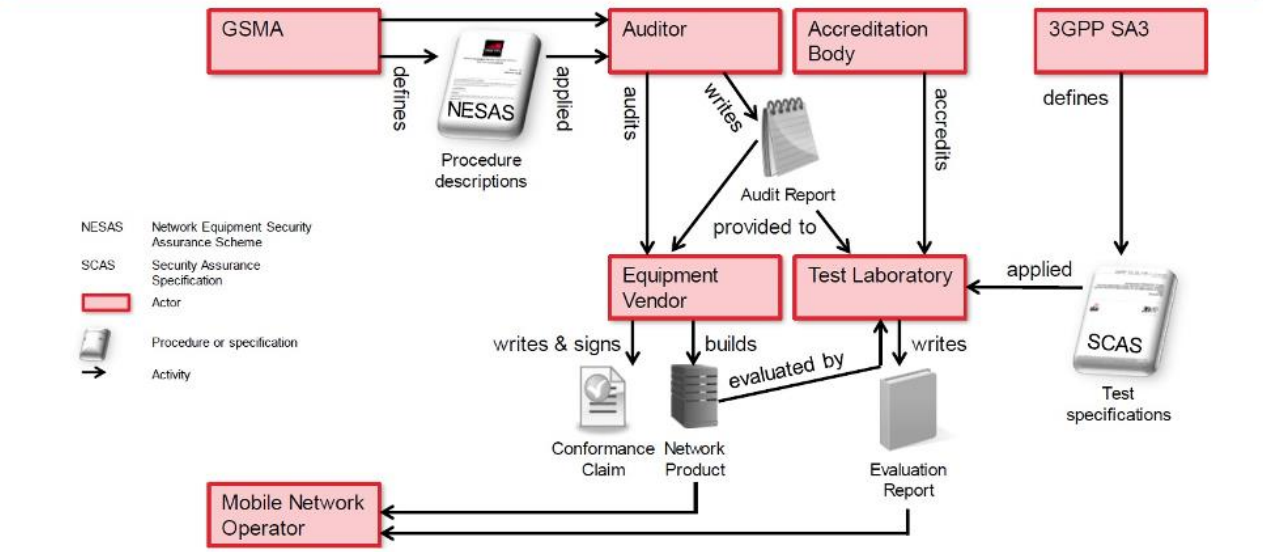

FIGURA 2.8 Il funzionamento del NESAS

Fonte: GSMA - 2019

La valutazione del prodotto, invece, viene condotta da laboratori certificati da GSMA, che applicano test di sicurezza standardizzati e predefiniti. Nel dettaglio, le specifiche per i test vengono definite dal 3GPP, mentre GSMA (oltre alla valutazione delle procedure per l'accreditamento del laboratorio di prova) fornisce i requisiti e la metodologia per l'Auditor. Quest'ultimo si occupa di effettuare l'*assessment* sul fornitore di apparecchiature e sulle sue procedure. In primo luogo, quindi, il vendor viene valutato dall'Auditor. Dopo essere stato audito, questi ha la possibilità di creare un nuovo prodotto migliorato da portare ad uno dei laboratori certificati per i test.

Il laboratorio, a sua volta:

1. viene accreditato[37] secondo una procedura stabilita dal NESAS;
2. utilizza le SCASes, specifiche per i test pubblicati dal 3GPP, per la valutazione;
3. deve convalidare le prove provviste dal fornitore di apparecchiature che il prodotto sia stato costruito in conformità con l'audit precedente;
4. scrive un rapporto di valutazione.

[37] L'accreditamento viene concesso da un Accreditation Body ISO 17025 che determina se il laboratorio è in grado di eseguire i test sui prodotti di rete.

Un elemento di accelerazione per i vendor, inoltre, è costituito dal fatto di dover effettuare la valutazione delle procedure una sola volta nel caso in cui le procedure interne utilizzate siano le stesse per la realizzazione di molteplici prodotti finali.

In generale, essendo in gran parte realizzato dagli stessi operatori che compongono la filiera, il NESAS appare avere caratteristiche a misura delle esigenze del settore. Per le stesse ragioni, grazie alla velocità con cui viene realizzata la procedura sia per i nuovi prodotti, sia per le versioni aggiornate dei prodotti esistenti, appare maggiormente applicabile. Inoltre, grazie a ulteriori rilasci, ai continui rapporti con gli stakeholder e alla continua raccolta di feedback, lo standard è progettato per evolversi nel tempo. Inoltre, è importante osservare che lo schema NESAS si basa sulla partecipazione volontaria, e i fornitori di apparecchiature liberi di decidere di seguire o meno lo schema. In questo senso, GSMA lascia quindi che sia il mercato a decidere, tramite l'adozione o meno dello schema, il successo o l'insuccesso dell'operazione.

Tra i vantaggi della diffusione del NESAS sottolineati da GSMA si evidenziano:

- per i vendor, evitare la moltiplicazione dei requisiti di sicurezza cui conformare le proprie apparecchiature e incrementare le capacità interne di migliorare e mantenere livelli di sicurezza adeguati;
- per gli operatori di rete, il venir meno della necessità di sviluppare specifici requisiti di sicurezza, che vengono realizzati su base associativa (all'interno di GSMA) e quindi dividendosi i costi;
- per i governi e le autorità nazionali, l'universale applicabilità del sistema di sicurezza e la possibilità di farlo interfacciare con le certificazioni nazionali, se necessario innalzando ulteriormente il livello di sicurezza.

L'iniziativa di GSMA è complementare al *toolbox* lanciato a gennaio 2020 dall'ENISA per creare un approccio comune tra i Paesi EU alla cybersecurity[38]. Inoltre, agosto 2020, GSMA ha annunciato che le imprese leader nel mercato delle apparecchiature di rete, Ericsson, Huawei, Nokia and ZTE, hanno completato con successo l'assessment dei propri processi di gestione di gestione dei prodotti e del loro ciclo di vita, ovvero la prima fase del NESAS.

[38] https://www.gsma.com/gsmaeurope/safer-mobile-use/latest-news/the-gsma-will-work-with-enisa-to-secure-5g-networks/#:~:text=The%20GSMA%20initiatives%20support%20efforts,tests%20the%20components%20for%20security.

Nella seconda fase di NESAS, i fornitori presenteranno i propri prodotti (apparecchiature di rete) ai laboratori qualificati per la valutazione. I laboratori eseguiranno i test di sicurezza definiti da 3GPP e controlleranno che i prodotti sottoposti a valutazione siano stati sviluppati in conformità con i processi di sviluppo e gestione del ciclo di vita valutati. La valutazione si concluderà con la produzione, da parte del laboratorio di prova, di un rapporto di valutazione, in cui verranno registrati i risultati del test. Il report viene reso disponibile al fornitore che può a sua volta girarlo ai propri clienti e ad altri stakeholder a sua discrezione.

3. LA SICUREZZA DELLE RETI TRA DISCIPLINA COMUNITARIA E INIZIATIVE NAZIONALI

3.1. DALLA DIRETTIVA NIS, AL CYBERSECURITY ACT, AL PACCHETTO DI STRUMENTI DELL'UE PER LA SICUREZZA DELLE RETI 5G. LO STATO DELL'ARTE NELL'UNIONE EUROPEA

L'implementazione delle reti 5G rappresenterà **l'elemento abilitante di un'ampia gamma di servizi** essenziali per il funzionamento del mercato interno e la gestione di funzioni di rilevanza cruciale per la società e l'economia, come la sanità, l'energia, i trasporti, i servizi finanziari, la produzione, fino ad arrivare all'organizzazione dei processi democratici. Si tratta di un'evoluzione di straordinaria rilevanza che si incardina, tuttavia, in un contesto che già da anni ha visto trasferire nel mondo digitale molte delle tradizionali attività socio-economiche rispetto alle quali si è palesata la necessità di apprestare adeguati strumenti di sicurezza. E infatti, considerata l'assoluta necessità di assicurare la **continuità e la sicurezza dei servizi digitali** e la **tutela dei diritti degli utenti**, in considerazione del carattere sovranazionale delle possibili minacce che possono riguardare le reti e gli stessi servizi, le istituzioni europee sono da molti anni impegnate al fine di accrescere la sicurezza degli utilizzatori di internet e dei servizi digitali e creare un ecosistema improntato sulla fiducia. La strategia lanciata nel 2013, in particolare, perseguiva l'obiettivo di rafforzare la resilienza informatica, ridurre il cyber crimine, sviluppare una politica europea di cybersecurity, accrescere le risorse industriali e tecnologiche per la sicurezza informatica e delineare una politica europea sulla cybersecurity coerente a livello internazionale.

Il vero punto di svolta nel panorama europeo è rappresentato, tuttavia, dall'adozione, il 6 luglio 2016, della **direttiva 2016/1148 (la cosiddetta direttiva NIS)**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, con la quale le istituzioni europee hanno affrontato le sfide in materia di cyber sicurezza, rivoluzionando la resilienza e la cooperazione in Europa.

In considerazione dell'assoluta centralità assunta, nella società odierna, dalle reti e dai sistemi e dai servizi informativi e della conseguente necessità di garantire che essi siano sicuri ed affidabili anche in un logica di garanzia della continuità delle attività socio-economiche, la direttiva obbliga gli Stati membri ad adottare una **strategia nazionale** in materia di sicurezza della rete e dei sistemi informativi (di cui la stessa direttiva, all'art. 7, individua i contenuti essenziali), istituisce un **gruppo di cooperazione** (composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA) con il compito di svolgere i propri compiti (in quattro ambiti, e nello specifico, pianificazione, guida, segnalazione e condivisione) sulla base di programmi di lavoro biennali, crea una rete di gruppi di

intervento per la **sicurezza informatica**, stabilisce **obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali** (tra cui l'obbligo di dotarsi di misure di sicurezza che comprendono prevenzione dei rischi, garanzia circa la sicurezza dei sistemi, delle reti e delle informazioni e capacità di gestire gli incidenti cui si aggiunge, per i secondi, la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i test e la conformità a norme internazionali).

La direttiva NIS, all'art. 23, prevede un riesame periodico da parte della Commissione circa il funzionamento della stessa e fissa al 9 maggio 2021 la formulazione della prima relazione a Parlamento europeo e Consiglio. A tal fine, la Commissione, a decorrere dal 25 giugno 2020, ha ufficialmente aperto la **consultazione pubblica relativamente alla futura revisione della direttiva NIS,** aperta a tutti i cittadini e gli stakeholder chiave dei settori di riferimento, oltre che agli enti istituzionali all'interno dei singoli Stati membri. Si tratta di una procedura di particolare rilevanza ove si consideri che a soli tre anni dalla sua attuazione, lo scenario della cybersecurity è cambiato radicalmente e che la pandemia ancora in atto ha mostrato con particolare vigore l'importanza di assicurare un ecosistema aperto e sicuro nel quale favorire l'interazione tra aziende, cittadini e pubbliche amministrazioni.

Ebbene, tale procedura, conclusasi il 2 ottobre scorso, perseguiva l'obiettivo di valutare il livello di funzionamento della Direttiva NIS all'interno di ciascun Paese dell'Unione attraverso lo studio del livello qualitativo e quantitativo della sicurezza delle reti e dei sistemi informativi degli Stati membri, la determinazione dell'efficacia, efficienza, coerenza e pertinenza della Direttiva NIS in considerazione dei progressi tecnologici e dell'evoluzione delle relative minacce informatiche, l'individuazione e la quantificazione dei costi e dei benefici, diretti e indiretti, derivanti dal processo di revisione della normativa nonché l'individuazione delle questioni chiave esistenti e di quelle potenzialmente emergenti a livello di sicurezza in grado di impattare sul funzionamento della direttiva.

Il 13 agosto scorso si è chiuso il primo step della consultazione pubblica all'esito del quale la Commissione ha raccolto le prime **opinioni** funzionali di alcuni dei principali attori coinvolti sulla attuazione e sull'impatto di potenziali modifiche al pacchetto normativo della Direttiva NIS. Il quadro che è emerso fotografa ancora una forte disuguaglianza e inefficienza degli strumenti di sicurezza informatica di cui si sono dotati gli Stati membri in relazione a quanto disposto dalla Direttiva e, conseguentemente, la necessità di ridurre la frammentazione normativa per favorire la

creazione di condizioni di parità indispensabili per l'ulteriore sviluppo del mercato unico. Dalle posizioni espresse emerge l'importanza e l'efficacia dei meccanismi di cooperazione transnazionale, inter-organizzativa e delle piattaforme di collaborazione create dalla direttiva NIS, come la rete di CSIRT/CERT europei e, al contempo, l'opportunità di intraprendere interventi migliorativi per colmare quel divario di sicurezza necessario a fronteggiare ogni tipo di minaccia cibernetica e favorire una più ampia condivisione di informazioni su minacce informatiche, vulnerabilità e incidenti.

A fronte di questioni ritenute ancora inadeguatamente trattate, sono state formulate specifiche richieste che si sostanziano nella richiesta di maggiore chiarezza ed uniformità nel processo che regola l'identificazione in ciascuno Stato degli operatori pubblici e privati di servizi essenziali (gli OES) e dei servizi digitali (FSD) ovvero di quelle persone giuridiche che fruiscono servizi quali cloud computing, e-commerce e motori di ricerca con sede (o rappresentanza) sul territorio nazionale, nell'inclusione, nell'ambito applicativo della direttiva, di soggetti ad oggi esclusi come alcuni ospedali ed operatori sanitari operanti nel settore sanitario che attualmente non possono essere identificati come parte di infrastrutture critiche oppure i social network, nonché la definizione di una metodologia comune al fine di assicurare un omogeneo livello di sicurezza cyber agli operatori ferroviari che svolgono la propria attività nei Paesi dell'Unione. A ciò si aggiunge la richiesta di dimostrare che gli operatori di telecomunicazione effettuino acquisti da fornitori sicuri, controllando la filiera di approvvigionamento tramite un approccio di *security by design* e la proposta di mirare al raggiungimento di un livello di protezione tale per cui i costi di un attacco cyber superino quelli degli eventuali danni provocati con l'attacco stesso, anche mediante l'adozione di sistemi operativi con moduli separati uno dall'altro che non possono comunicare se non con capacità molto limitate.

Se la direttiva NIS, per la prima volta, è intervenuta a disciplinare in maniera organica il tema della sicurezza delineando la cornice normativa ed organizzativa nell'UE e rinsaldando la cooperazione tra stati membri e istituzioni, attenzione al tema della sicurezza delle reti e dei servizi è stata riposta anche nel **Codice europeo delle comunicazioni elettroniche di cui alla direttiva 2018/1972** i cui artt. 40 e 41 sono specificamente dedicati all'argomento. Tali disposizioni, in particolare: 1) pongono a carico degli Stati membri il compito di assicurare che i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico adottino misure adeguate e proporzionate di natura tecnica e organizzativa per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi; 2) attribuiscono all'ENISA – di cui si parlerà più

approfonditamente *infra* – la funzione di facilitatore del coordinamento tra gli Stati membri, al fine di evitare l'esistenza di requisiti nazionali divergenti che possano comportare rischi per la sicurezza e creare ostacoli al mercato interno; 3) prescrivono agli Stati membri di assicurare che i fornitori di reti pubbliche di comunicazioni elettronica o di servizi di comunicazione elettronica accessibili al pubblico comunichino senza indebito ritardo all'autorità competente ogni incidente di sicurezza che abbia avuto conseguenze significative sul funzionamento delle reti o dei servizi; 4) individuano i parametri da considerare per determinare la rilevanza dell'impatto di un incidente di sicurezza (numero di utenti interessati dall'incidente di sicurezza, durata dell'incidente di sicurezza, diffusione geografica della zona interessata dall'incidente di sicurezza, misura in cui è colpito il funzionamento della rete o del servizio, portata dell'incidenza sulle attività economiche e sociali); 5) prevedono la trasmissione annuale, da parte dell'autorità competente interessata alla Commissione e all'ENISA, di una relazione sintetica delle notifiche ricevute e delle azioni adottate; 6) prescrivono agli Stati membri di provvedere affinché, in caso di minaccia particolare e significativa di incidenti di sicurezza nelle reti pubbliche di comunicazione elettronica o nei servizi di comunicazione elettronica accessibili al pubblico, i fornitori di tali reti o servizi informino gli utenti potenzialmente interessati da tale minaccia di eventuali misure di protezione o rimedi cui possono ricorrere; 7) attribuiscono alla Commissione, con il parere dell'ENISA, il potere di adottare atti di esecuzione che descrivano dettagliatamente le misure tecniche e organizzative nonché le circostanze, il formato e le procedure che si applicano agli obblighi di notifica fatta salva sempre la possibilità per gli Stati membri di adottare ulteriori prescrizioni; 8) dispongono che gli Stati membri assicurino alle autorità competenti la facoltà di imporre ai fornitori di reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico di fornire le informazioni necessarie per valutare la sicurezza delle loro reti e dei loro servizi, in particolare i documenti relativi alle politiche di sicurezza e sottostare a una verifica della sicurezza effettuata da un organismo qualificato indipendente o dall'autorità competente mettendo a disposizione dell'autorità competente i risultati di tale verifica e sostenendo l'onere finanziario della verifica stessa; 9) prescrivono agli Stati membri di assicurare alle autorità competenti tutti i poteri necessari per indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza delle reti e dei servizi nonché il potere di ottenere assistenza da un gruppo di intervento per la sicurezza informatica in caso di incidente («CSIRT») designato ai sensi dell'articolo 9 della direttiva (UE) 2016/1148 in relazione alle questioni che rientrano nei compiti dei CSIRT.

Centrale, nel sistema delineato dalla disciplina europea, il ruolo dell'ENISA i cui obiettivi, compiti ed aspetti organizzativi sono stati disciplinati dal **Regolamento n. 881/2019** del 17 aprile 2019

(noto come "*Cybersecurity Act*"), il quale, al fine di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cybersicurezza, cyberresilienza e fiducia all'interno dell'Unione, ha inoltre fissato un quadro per l'introduzione di **sistemi europei di certificazione della cybersecurity** in grado di garantire un livello adeguato di cybersecurity dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersecurity nell'Unione. In particolare, mentre i primi 45 articoli disciplinano poteri, competenze ed organizzazione dell'ENISA, a partire dall'art. 46, il regolamento fissa il quadro europeo di certificazione della cybersecurity introducendo un approccio armonizzato dei sistemi europei di certificazione allo scopo di creare un mercato unico digitale per i prodotti, i servizi e i processi TIC.

La procedura delineata dal Regolamento prevede, inoltre, che la Commissione, sulla base della proposta di sistema preparata dall'ENISA, possa adottare atti di esecuzione, che almeno ogni cinque anni l'ENISA valuti ogni sistema europeo di certificazione della cybersecurity adottato, tenendo conto del riscontro ricevuto dalle parti interessate e che, se necessario, la Commissione o il Gruppo europeo per la certificazione della cybersecurity (ECCG, di cui si dirà *infra*) possa chiedere all'ENISA di avviare il processo di sviluppo di una proposta riveduta di sistema.

Il Regolamento individua poi, con particolare rigore, un'ampia gamma di obiettivi di sicurezza connessi all'istituzione dei sistemi europei di certificazione e suddivide in tre, sulla base del livello di rischio associato al previsto uso del prodotto, servizio o processo TIC, in termini di probabilità e impatto di un incidente, i livelli di affidabilità dei prodotti, servizi e processi TIC: **di base, sostanziale ed elevato**, declinando, in riferimento a ciascuno dei tre livelli, le specifiche attività di valutazione previste nonché il ricorso ad attività sostitutive di effetto equivalente qualora le attività di valutazione previste non siano appropriate. Il Regolamento prescrive, a livello organizzativo, la designazione, da parte degli Stati membri, di una o più autorità nazionali di certificazione della cybersecurity nel proprio territorio oppure, con l'accordo di un altro Stato membro, la designazione di una o più autorità nazionali di certificazione della cybersecurity stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.

Il medesimo regolamento istituisce il **Gruppo europeo per la certificazione della cybersecurity**, composto da rappresentanti delle autorità nazionali di certificazione della cybersecurity o da rappresentanti di altre autorità nazionali competenti, con compiti di assistenza, proposta, collaborazione e consulenza nei rapporti con la Commissione ed ENISA. Quanto alla valutazione

dell'impianto normativo introdotto, il regolamento prevede che entro il 28 giugno 2024, e successivamente ogni cinque anni, la Commissione valuti l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie.

L'esigenza di implementare efficaci standard di sicurezza assume rilevanza peculiare con riguardo alle reti 5G proprio in considerazione dell'ampia serie di servizi digitali che abiliteranno e la conseguente necessità di scongiurare le gravi ed impattanti conseguenze di malfunzionamenti sistemici e diffusi. Partendo da tali constatazioni e dal desiderio di far rivestire all'Unione europea un ruolo da leader a livello mondiale, la Commissione europea, il 26 marzo 2019 ha adottato la **Raccomandazione n. 2019/534** sulla cybersecurity delle reti 5G con la quale ha evidenziato i rischi di cybersecurity rispetto a tali reti e presentato orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi. In particolare, per affrontare i rischi di cybersecurity nelle reti 5G, il documento pone in evidenza la necessità di considerare non solo i **fattori tecnici**, ma anche **fattori ulteriori e diversi** come, ad esempio, requisiti normativi o di altro tipo imposti ai fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione, il modello di governance esistente nel Paese analizzato, il rischio generale di influenza da parte di un Paese terzo, l'assenza di accordi di cooperazione sulla sicurezza o di disposizioni analoghe, quali le decisioni di adeguatezza, tra l'Unione e il Paese terzo interessato per quanto riguarda la protezione dei dati, etc.

La raccomandazione individua, inoltre, un **set di azioni** tese a consentire, a livello nazionale ed europeo, un'adeguata valutazione dei rischi e a individuare un'eventuale serie comune di misure da adottare per attenuare i rischi di cybersecurity relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare le reti 5G ed individua una **roadmap** chiara e stringente secondo cui gli Stati membri avrebbero dovuto valutare i rischi, aggiornare i requisiti di sicurezza e i metodi di gestione dei rischi applicati alle reti 5G, aggiornare i pertinenti obblighi imposti alle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico.
Per un'efficace azione di prevenzione e contrasto delle minacce, il documento sottolinea l'importanza di porre in essere una valutazione dei rischi coordinata a livello europeo mediante lo scambio di informazioni tra gli Stati e con gli organismi pertinenti dell'Unione al fine di sviluppare

una consapevolezza comune dei rischi di cybersecurity esistenti e potenziali associati alle reti 5G. A tal fine, gli Stati membri avrebbero dovuto, inoltre, trasmettere le valutazioni nazionali dei rischi alla Commissione e all'Agenzia dell'Unione europea per la cybersecurity (ENISA) entro il 15 luglio 2019 così da consentire a quest'ultima di completare una mappatura specifica del panorama delle minacce per le reti 5G. Tutto ciò considerato, la raccomandazione individuava una serie di step temporalmente scanditi per giungere a una revisione congiunta dell'esposizione a livello di Unione ai rischi relativi alle infrastrutture alla base dell'ecosistema digitale, redigere un inventario dei tipi di rischi di sicurezza che possono incidere sulla cybersecurity delle reti 5G e identificare una serie di possibili misure di attenuazione. Infine, la raccomandazione invita gli Stati membri a cooperare con la Commissione per valutare gli effetti di quanto previsto dalla stessa, entro il 10 ottobre 2020, al fine di determinare le modalità di azione.

Ebbene, al fine di dare attuazione a quanto previsto nella raccomandazione appena descritta, il **9 ottobre 2019** è stata pubblicata dal gruppo di cooperazione NIS, composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA, una **relazione sulla valutazione coordinata a livello di UE dei rischi per la cibersicurezza delle reti di quinta generazione** la quale, partendo dai risultati delle valutazioni nazionali dei rischi per la cibersicurezza, effettuate da tutti gli Stati membri dell'UE, ha individuato le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici. In particolare, nell'individuare le più importanti sfide per la sicurezza che possono manifestarsi o acuirsi (rispetto alle reti precedenti) con l'avvento delle reti 5G, tale relazione si concentra, da un lato, sulle innovazioni abilitate da tali reti (con riguardo sia al software che alle numerose applicazioni e servizi resi possibili dal 5G) e, dall'altro, al ruolo dei fornitori nella realizzazione e nell'uso delle reti 5G nonché al grado di dipendenza da singoli fornitori.

Tale documento, dopo aver riportato un'analisi del contesto, ha evidenziato le specifiche tecniche associate alla tecnologia 5G. In seguito, vengono identificati e descritti nel dettaglio gli asset utilizzati per il 5G, individuando per ciascuno gli impatti potenziali in termini di perdita di riservatezza, integrità e disponibilità. Viene quindi proposta una tassonomia delle minacce che possono coinvolgere la tecnologia 5G associando ciascuna alle capacità di specifici attori (entità statuali, cyber criminali, hacktivisti, ecc.). Sulla base dell'analisi effettuata vengono quindi proposte alcune raccomandazioni per i Paesi membri, per gli stakeholder del mercato 5G e per le autorità nazionali competenti sul tema di sicurezza del 5G. Ad integrazione del rapporto degli Stati membri dell'UE sulle valutazioni del rischio a livello dell'UE sulla sicurezza 5G appena descritto, il **21**

novembre 2019, l'ENISA ha pubblicato un *Threat Landscape for 5G Networks*, valutando le minacce legate alle reti 5G. Si tratta di un rapporto interessante nel quale, sulla base anche del contributo offerto da gruppi e organismi di standardizzazione 5G e stakeholder 5G come operatori, fornitori, organizzazioni nazionali e internazionali, sono state individuate le sfide e le possibili minacce nella sicurezza delle reti 5G, è stato definito un diagramma degli asset, formulata una tassonomia delle minacce, identificata l'esposizione dei diversi asset e valutate le motivazioni dell'agente di minaccia.

Anche il Consiglio, nelle proprie conclusioni del **3 dicembre 2019,** ha appoggiato i rilievi formulati dal gruppo di cooperazione NIS, sottolineando l'importanza di adottare un approccio coordinato e di assicurare un'efficace attuazione della raccomandazione – mediante adozione di tutte le misure necessarie nell'ambito delle rispettive competenze per garantire la sicurezza e l'integrità delle reti di comunicazione elettronica, in particolare le reti 5G – al fine di evitare la frammentazione del mercato unico.

Il **29 gennaio 2020** è stata infine pubblicata dalla Commissione la Comunicazione ***"Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE"*** nella quale, preso atto dell'assoluta rilevanza del 5G per molti servizi essenziali e, dunque, della strategica necessità per l'Unione di garantire la cybersecurity delle reti 5G in un momento in cui gli attacchi informatici sono in aumento, più sofisticati che mai e ad opera di un'ampia gamma di soggetti, viene dato conto di come nell'ambito della cooperazione NIS e, a seguito del completamento da parte degli Stati membri delle procedure di valutazione dei rischi delle proprie infrastrutture di rete 5G, il gruppo di cooperazione NIS abbia pubblicato una relazione sulla valutazione dei rischi coordinata a livello dell'UE sulla cybersecurity di tali reti in cui sono state individuate le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo) che interessano le reti 5G.

Nella medesima data lo stesso gruppo di cooperazione NIS ha pubblicato il **pacchetto di strumenti dell'UE** (**Toolbox sul 5G**) comprendente misure di attenuazione dei rischi, che tratta tutti i rischi individuati nella relazione coordinata sulla valutazione dei rischi individuando e descrivendo una serie di misure strategiche e tecniche, nonché di corrispondenti azioni di sostegno volte a rafforzare la loro efficacia, che possono essere attuate per attenuare i rischi individuati. Il documento, in particolare, nell'evidenziare come l'Europa sia una delle regioni più avanzate nel mondo in relazione al lancio commerciale dei servizi 5G (entro la fine del 2020, infatti, i primi servizi 5G

dovrebbero essere disponibili in 138 città europee), fa il punto su alcuni dei settori rispetto ai quali il 5G opererà quale fattore abilitante una serie di importanti applicazioni e, nello specifico***, eHealth*** (con riguardo da un lato, alla possibilità di monitorare a distanza dello stato di salute dei pazienti e delle loro cartelle e di formulare una diagnosi intelligente e, dall'altro, all'impiego di robot in ausilio dei medici nell'ottica di migliorare le performance mediche), **reti energetiche intelligenti** (ad alta efficienza, con minori interruzioni di servizio su piccola scala e con installazioni più semplici e dal minor impatto ambientale), **fabbriche del futuro** (con monitoraggio a distanza di processi e macchinari), **media ed intrattenimento** (con riferimento, in particolare, allo sviluppo di applicazioni come la realtà virtuale e lo streaming video) e **mobilità** (con lo sviluppo della mobilità connessa e automatizzata con obiettivo zero incidenti e l'implementazione della connettività in tutte le modalità di trasporto).

L'obiettivo dichiarato dal documento è identificare un possibile insieme comune di misure in grado di mitigare i principali rischi per la sicurezza informatica delle reti 5G (così come sono stati identificati nella relazione di valutazione del rischio coordinata dall'UE) e fornire una guida per la selezione delle misure da adottare, al fine di creare un solido quadro di misure che garantisca un adeguato livello di sicurezza informatica delle reti 5G in tutta l'UE e un approccio coordinato tra gli Stati membri. Le misure presentate nel pacchetto contribuiscono al raggiungimento di una serie di importanti obiettivi di sicurezza che si autoalimentano e che rivestono grande rilevanza per affrontare i rischi identificati nel rapporto di valutazione dei rischi e proteggere la riservatezza, l'integrità e la disponibilità delle reti 5G. Tali obiettivi, nello specifico, si sostanziano: a) nel rafforzare la sicurezza nella progettazione, implementazione e funzionamento delle reti; b) innalzare gli standard di sicurezza di base per la sicurezza di prodotti e servizi; c) minimizzare l'esposizione ai rischi derivanti dal profilo di rischio dei singoli fornitori; d) evitare o limitare le principali dipendenze da un singolo fornitore nelle reti 5G; e) promuovere un mercato diversificato, competitivo e sostenibile per le apparecchiature 5G.

Dopo aver sinteticamente richiamato gli strumenti regolatori già esistenti nel diritto dell'Unione Europea (Direttiva NIS, *Cybersecurity Act*, il Reg. 452/2019 che ha istituito un quadro per il controllo degli investimenti esteri diretti nell'Unione, GDPR, Direttiva *ePrivacy* etc.), il documento evidenzia la crucialità degli operatori di rete mobile e dei loro fornitori, responsabili, questi ultimi, della fornitura del software e dell'hardware necessari per il funzionamento delle reti. Quanto alle misure identificate, il pacchetto identifica: 1) **8 misure strategiche**, comprendenti il rafforzamento dei poteri normativi delle autorità per l'esame dell'approvvigionamento e dello spiegamento della

rete, misure specifiche per affrontare i rischi legati a vulnerabilità non tecniche (ad esempio, rischio di interferenza da parte di un Paese terzo o rischi di dipendenza), nonché possibili iniziative per promuovere una catena di approvvigionamento e di valore 5G sostenibile e diversificata, al fine di evitare rischi sistemici di dipendenza a lungo termine; 2) **11 misure tecniche,** comprendenti misure per rafforzare la sicurezza delle reti e delle attrezzature 5G ed in particolare la sicurezza delle tecnologie, del software, dei processi, delle persone e dei fattori fisici.

A sostegno di tali misure, lo stesso documento individua una serie di azioni di supporto che si sostanziano, tra le altre, nel rivedere o sviluppare linee guida e best practice sulla sicurezza della rete, rinforzare le capacità di test e controllo a livello nazionale ed europeo, supportare la standardizzazione, scambiare le migliori pratiche sull'attuazione delle misure strategiche (in particolare le discipline nazionali per la valutazione del profilo di rischio dei fornitori), garantire che i progetti di implementazione del 5G sostenuti con finanziamenti pubblici tengano conto dei rischi per la sicurezza informatica ed assicurare l'applicazione di misure di sicurezza tecniche e organizzative standard attraverso uno specifico schema di certificazione a livello europeo. La sezione certamente più complessa del documento è rappresentata dal paragrafo 4.2 dove, per ciascuna delle nove aree di rischio identificate nella relazione sulla valutazione coordinata a livello di UE dei rischi, il pacchetto individua dei piani di mitigazione del rischio, consistenti nella combinazione di misure strategiche e/o tecniche (insieme ad appropriate azioni di supporto) che vengono classificate in quattro livelli, sulla base di una valutazione che considera il rischio da fronteggiare ed il rischio persistente dopo l'applicazione della stessa misura.

Nel tracciare le conclusioni, il pacchetto invita gli Stati membri ad attuare misure e disporre di poteri per attenuare i rischi, rafforzando i requisiti di sicurezza per gli operatori delle reti mobili, valutando il profilo di rischio dei fornitori, applicando restrizioni adeguate ai fornitori considerati ad alto rischio, comprese le necessarie esclusioni per gli asset critici, garantendo che ogni operatore disponga di un'adeguata strategia multifornitore per evitare o limitare l'eventuale forte dipendenza da un unico fornitore ed evitare la dipendenza da fornitori considerati ad alto rischio.

La Commissione, nel manifestare la propria volontà di continuare a fornire pieno sostegno e intraprendere tutte le azioni pertinenti nell'ambito delle proprie competenze, al fine di sostenere l'attuazione del pacchetto di strumenti da parte degli Stati membri e di rafforzarne l'impatto, ha invitato questi ultimi a delineare, entro il 30 aprile 2020, azioni concrete e misurabili per attuare la serie di misure chiave raccomandate nelle conclusioni del pacchetto di strumenti dell'UE. Li ha

invitati inoltre a preparare, entro il 30 giugno 2020, una relazione del gruppo di cooperazione NIS sullo stato di attuazione in ciascuno Stato membro di tali misure chiave, in base alle relazioni presentate e al monitoraggio effettuato periodicamente, in particolare nell'ambito del gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA.

Ebbene, il 24 luglio il gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, ha pubblicato una relazione sui progressi degli Stati membri nell'attuazione del *Toolbox* sulla sicurezza 5G. Si tratta di un documento molto interessante nel quale si fa il punto sul livello di maturità raggiunto dai vari Paesi nell'implementazione delle misure contenute nel *Toolbox.* Sintetizzando le posizioni espresse dai singoli Stati membri, il documento rileva come tutti abbiano avviato un processo di revisione e rafforzamento delle misure di sicurezza in vista del 5G, anche se in alcuni Paesi i lavori sono ancora in corso e non sono state dunque ancora adottate misure definitive.

A livello generale, la relazione sottolinea come i tre principali rischi individuati siano quello dell'errata configurazione delle reti, della mancanza di controllo all'accesso e di interferenze statali attraverso la catena di fornitura 5G. Rispetto a tale ultimo rischio, in particolare, considerando quanto espresso dagli Stati circa l'efficacia di contrasto delle misure esistenti, il dato che emerge è la convinzione degli Stati circa la mancanza di misure esistenti adeguate. Più in dettaglio, con riferimento alle misure strategiche, la relazione riporta un livello di maturità medio-alto nel rafforzamento del ruolo e dei poteri delle autorità regolatorie (nella grande maggioranza dei Paesi sono già state intraprese o concluse iniziative in tale senso mentre in altri sono previste entro la fine del 2020 o il 2021), mentre con specifico riguardo all'esecuzione di audit e la richiesta di informazioni agli operatori il livello di maturità raggiunto è definito medio. In relazione al tema dei fornitori ad alto rischio e alle possibili interferenze da parte di Stati terzi, il documento rileva, in generale, una diffusa consapevolezza della delicatezza della questione e, a fronte di ciò, un grado di implementazione medio, evidenziando come nella maggioranza degli Stati siano in atto procedure – piuttosto complesse, visti i potenziali impatti socio-economici – tese a introdurre specifiche misure.
Con riguardo al tema della dipendenza da singoli fornitori, la relazione da atto, in generale, della complessità del tema, della necessità di comprendere il coinvolgimento dei diversi fornitori rispetto ai singoli elementi della rete, della difficoltà tecnica ed operativa di applicare una strategia *multi-vendor* in determinati punti della rete, del limitato numero di fornitori 5G, delle maggiori criticità per i Paesi più piccoli, dei possibili effetti sugli operatori conseguenti alla formulazione di richieste

diversificate ai fornitori e della necessità di individuare basi normative specifiche che consentano di imporre determinati obblighi a carico dei fornitori.

Interessanti anche le considerazioni relative all'implementazione di misure tese a garantire la sicurezza delle reti 5G. Sul punto, in particolare, il documento, dopo aver definito medio-basso il livello di maturità raggiunto nell'implementazione di tali misure, descrive un panorama piuttosto diversificato nel quale emerge, tuttavia, la richiesta, proveniente da molti Stati membri, di un approccio coordinato a livello europeo in materia di standard. Fotografata la situazione generale, la relazione sottolinea l'importanza di intensificare gli scambi di informazioni, best pratice e soluzioni tra Stati membri e la cooperazione con la Commissione per l'implementazione del *Toolbox* e lo sviluppo di standard e schemi di certificazione europei. Entro il 1° ottobre 2020 gli Stati membri, in collaborazione con la Commissione, dovranno stabilire l'eventuale necessità di ulteriori azioni.

3.2. LA TUTELA DELLA SICUREZZA DELLE RETI NEI MAGGIORI PAESI EUROPEI

Osservando l'orientamento dei maggiori Paesi europei emerge come, nell'approccio alla sicurezza delle reti di telecomunicazione e del 5G, siano stati generalmente tenuti in considerazione **due principi**: la necessità di non mettere a rischio la realizzabilità di progetti ritenuti essenziali per lo sviluppo delle nuove tecnologie e la tutela dei principi economici e commerciali praticati in Italia e nel mondo occidentale. Fino a pochi mesi fa risultava che quasi tutti i Paesi impegnati nel rafforzamento delle proprie misure di sicurezza e di vigilanza non avessero imposto esclusioni a priori all'ingresso di soggetti extraeuropei nello sviluppo e nella fornitura di prodotti e servizi relativi alle reti 5G[39]. Le circostanze sono tuttavia mutate a causa delle **pressioni provenienti dagli USA** sui Paesi dell'alleanza NATO, diventate più esplicite determinando un maggiore irrigidimento di diversi Paesi europei. In particolare, nel luglio 2020 la Gran Bretagna ha ufficializzato la decisione di escludere Huawei dalle forniture per la nuova rete 5G del Paese dal 31 dicembre 2020, mentre, nell'ottobre 2020, anche la Svezia ha ufficializzato il divieto sulle compagnie cinesi Huawei e ZTE in vista dell'asta per l'aggiudicazione delle frequenze legate alla connettività 5G prevista, per il novembre dello stesso anno. L'autorità svedese (PST), inoltre, ha imposto la rimozione di tutte le apparecchiature 5G di Huawei e ZTE entro il 1° gennaio 2025. Nella stessa direzione si è mosso

[39] Rispetto a tale contesto fanno parzialmente eccezione Polonia e Romania, che hanno sottoscritto dichiarazioni congiunte con gli Stati Uniti. A livello extra-europeo, una linea di restrizione verso il coinvolgimento di aziende cinesi nella implementazione del 5G è stata anche adottata da Australia, Nuova Zelanda e Giappone.

anche il Belgio, la cui capitale, essendo sede dei quartieri generali della NATO e dell'Unione Europea, è considerata strategicamente importante dagli Stati Uniti. Gli operatori belga Orange e Proximus hanno infatti affidato la costruzione della rete 5G alla compagnia finlandese Nokia, di fatto escludendo i rivali asiatici. Una risposta significativa è stata prodotta anche dal Parlamento Europeo, dove, con una lettera inviata ai commissari Breton, Vestager e Dombrovskis, quarantuno eurodeputati provenienti da cinque gruppi differenti hanno dichiarato come i fornitori extraeuropei rappresentino "un pericolo per la sicurezza" dei network comunitari.[40]

Attualmente, nei quattro maggiori Paesi europei oltre all'Italia **si rilevano approcci differenti**: diversificazione e restrizione dell'accesso alla rete agli operatori extra-europei in Gran Bretagna; approccio caso per caso in Francia; rafforzamento dei poteri del Governo in Spagna; rafforzamento della protezione di investimenti ed acquisti esterni nelle aziende tecnologiche e approvazione di dettagliati criteri di sicurezza validi per tutti gli operatori in Germania.

3.2.1 Germania

La legge tedesca, al fine di tutelare gli asset tecnologici nazionali, prevede la possibilità per il Governo di esercitare il potere di veto sugli acquisti di una quota azionaria superiore al 10% delle aziende che hanno sede in Germania. Seguendo lo stesso principio il Paese si è inoltre reso promotore, insieme alla Francia, dell'adozione di un nuovo sistema di verifica UE degli investimenti di soggetti extra-europei che abbiano come obiettivo le aziende comunitarie. A tal proposito, si osserva come la volontà tedesca di proteggere le proprie tecnologie strategiche si rifletta anche nel dibattito interno sullo sviluppo della rete 5G. A febbraio 2020, il Governo ha avallato un position paper[41] che raccomanda regole più severe per i *vendor* extra-UE. Nello specifico viene consigliato l'utilizzo di un approccio *multivendor* e l'applicazione di criteri di sicurezza particolarmente stringenti per i componenti sensibili della rete[42].

[40] Lettera sottoscritta a Bruselles il 14 ottobre 2020.
[41] https://www.euractiv.de/wp-content/uploads/sites/4/2020/02/Positionspapier_5G.pdf?_ga=2.176762789.1647555648.1584975099-1808829908.1584975099
[42] Il documento è stato redatto dai leader della CDU per rispondere alle preoccupazioni di alcuni esponenti del partito, che vedono nell'ingresso di vendor extra-europei un incremento del livello di rischio per la sicurezza nazionale, ed ha lo scopo di gettare le basi affinché il governo di coalizione della Cancelliera Merkel adotti una posizione comune sul 5G dopo mesi di dibattiti divisori.

La Federal Network Agency (BNetzA) ha pubblicato nel 2019 un documento[43] contenente i principi chiave per il prossimo aggiornamento dei requisiti di sicurezza delle reti di telecomunicazioni. Le linee guida sono state sviluppate in accordo con l'Ufficio federale per la sicurezza delle informazioni (BSI) e il Commissario federale per la protezione dei dati e la libertà di informazione (BfDI). Secondo quanto emerge dal documento, in considerazione dell'importanza del 5G per la futura competitività nazionale, l'hardware e il software utilizzati per la rete di quinta generazione devono soddisfare i più elevati standard di sicurezza esistenti. In sintesi, il documento prevede che:

- i sistemi possono essere acquistati solo da fornitori affidabili che indubbiamente rispettano le norme di sicurezza nazionali nonché le norme sul segreto delle telecomunicazioni e sulla protezione dei dati;
- il traffico di rete deve essere monitorato regolarmente e continuamente per rilevare eventuali anomalie e, in caso di dubbio, devono essere adottate misure adeguate a proteggerlo;
- i componenti di rete e di sistema rilevanti per la sicurezza[44] possono essere utilizzati solo se sono stati certificati come sicuri da un ente incaricato dall'Ufficio federale per la sicurezza delle informazioni;
- i componenti di rete e di sistema rilevanti per la sicurezza possono essere ottenuti solo da *vendor* affidabili;
- i componenti di rete e di sistema rilevanti per la sicurezza possono essere utilizzati solo dopo un adeguato test di collaudo alla consegna e devono essere sottoposti a controlli di sicurezza regolari e continui;
- è necessario dimostrare che l'hardware e il software testato sia effettivamente utilizzato nei prodotti installati;
- nella costruzione delle reti è preferibile evitare di affidarsi ad un solo v*endor*.

Al fine di dare valenza legale a questi requisiti, il Governo Federale intende inserirli nella prossima modifica della sezione 109 della legge sulle telecomunicazioni (109 Absatz 6 Satz 1 TKG).

[43] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2

[44] La definizione di componenti rilevanti per la sicurezza viene fatta di comune accordo tra BNetzA e BSI.

Analizzando le strategie dei principali operatori, risulta che l'ex-incumbent Deutsche Telekom ha siglato a luglio[45] un accordo con Ericsson per la fornitura della parte RAN dei propri apparati 5G. Parallelamente, sia Vodafone che Telefónica hanno siglato accordi con i propri fornitori per le reti di quinta generazione, rispettivamente con Huawei ed Ericsson nel caso di Vodafone e con Nokia e Huawei nel caso di Telefonica.

Sebbene i principali operatori mobili in Germania abbiano dichiarato di **non condividere eventuali *ban* per nessun operatore**[46], a seguito della recente intervista della Cancelliera Merkel sul Financial Times[47], è emerso che il Governo tedesco starebbe preparando un progetto di legge per fine ottobre con l'obiettivo di **limitare l'utilizzo di componenti di *vendor* extra-europei** nelle reti nazionali 5G. In questo modo la Germania eviterebbe un divieto assoluto per Huawei e ZTE, ma, contemporaneamente, creerebbe ostacoli burocratici che potrebbero rivelarsi insormontabili per le aziende cinesi. Secondo le stime di Deutsche Telekom, Telefonica e Vodafone, una tale decisione non solo creerebbe difficoltà all'adeguamento e all'integrazione della nuova rete 5G sui già esistenti sistemi 4G, ma causerebbe anche un incremento dei costi pari a circa 50 miliardi di euro.

3.2.2 Spagna

Anche in Spagna sono state recentemente approvate delle norme volte a garantire al Governo il potere di intervenire sullo sviluppo delle reti 5G in territorio spagnolo. Il Regio decreto legislativo 14/2019[48] ha introdotto nella Legge sulle Telecomunicazioni[49] della Spagna alcune misure a tutela della pubblica sicurezza in materia di amministrazione digitale, appalti del settore pubblico e telecomunicazioni. In particolare, la rettifica all'articolo 6 ha conferito al Governo, su base eccezionale e transitoria, poteri di intervento speciali su qualsiasi infrastruttura, risorsa o elemento associato alle reti e ai servizi di comunicazione elettronica nel caso si verifichino circostanze che possono incidere sull'ordine pubblico e sulla sicurezza nazionale. Le circostanze che possono attivare l'intervento governativo sono:

[45] https://www.capacitymedia.com/articles/3826010/huawei-loses-to-ericsson-in-bid-for-deutsche-telekoms-5g-ran
[46] https://www.teletrader.com/deutsche-telekom-against-ban-on-huawei/news/details/52956701?internal=1&ts=1603966646771
[47] Articolo del 1° ottobre 2020
[48] https://www.boe.es/buscar/act.php?id=BOE-A-2019-15790#a6
[49] https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

- una minaccia immediata e grave all'ordine pubblico, alla pubblica sicurezza o alla sicurezza nazionale;
- una minaccia immediata e grave alla salute pubblica;
- una presunta attività illecita che può causare gravi danni al funzionamento dei servizi di pubblica sicurezza, protezione civile e di emergenza;
- una grave interferenza nei servizi e nelle reti di comunicazione elettronica;
- un'azione che crea danni economici o operativi ad altri fornitori o altri utenti dello spettro radio.

Le Pubbliche Amministrazioni spagnole devono inoltre informare il Ministero dell'Economia e degli Affari dell'avviamento di qualsiasi progetto per l'installazione di nuove infrastrutture di rete. All'interno del Paese non ci sono soggetti politici di rilievo che propendono per l'esclusione di *vendor* extra-europei ma, vista l'importanza strategica che avrà il 5G, l'Amministrazione ha comunque deciso di avviare una consultazione pubblica[50] con l'obiettivo di elaborare una norma che contenga requisiti di sicurezza specifici per le reti di quinta generazione.

Con la presentazione del piano di investimenti per il rilancio dell'economia a seguito della pandemia globale, il Governo spagnolo ha dichiarato l'obiettivo di una copertura 5G per il **75% del territorio nazionale entro fine 2020**. Per la realizzazione della nuova rete, il Governo **non escluderà le compagnie extraeuropee**, e, al contrario, ha dichiarato di voler fare affidamento sia su di esse che su diversi *provider* europei e americani.

Per quanto riguarda le decisioni prese dagli operatori, il gruppo Telefonica aveva annunciato a dicembre 2019 che la fornitura di apparecchiature di rete 5G sarebbe stata diversificata per evitare che un solo vendor avesse eccessivo potere contrattuale. Lo stesso principio della diversificazione sarebbe stato applicato anche alla rete core[51]. A settembre 2020 l'ex-incumbent ha tuttavia siglato un accordo con la sola Ericsson per l'implementazione della propria rete 5G in Spagna e, di conseguenza, le apparecchiature del fornitore svedese sono state estese a più di 400 città iberiche, coprendo il 40% del territorio nazionale con il servizio 5G nelle bande 3.5 GHz e 1.8-2.1 GHz.[52]

[50] https://avancedigital.gob.es/es-es/Participacion/Documents/proyecto-norma-ciberseguridad-5G.pdf

[51] A tal proposito, per ragioni di natura tecnica l'ex-incumbent ha espresso la volontà di ridurre l'impiego di componentistica Huawei, attuale fornitore della rete core 4G. https://www.cnbc.com/2019/12/17/reuters-america-telefonica-to-drastically-reduce-huawei-kit-for-its-core-5g-network.html

[52] https://www.rcrwireless.com/20201012/5g/telefonica-5g-network-reaches-450-spanish-cities-report

Anche Orange España, controllata spagnola dell'ex *incumbent* francese, ha siglato un accordo con il colosso svedese, e a oggi fornisce servizi 5G a Madrid e Barcellona operando sullo spettro di 3,6 GHz. Vodafone España, che offre la rete 5G in 21 città spagnole, ha invece deciso di adottare un approccio multi-vendor, rinnovando per il 5G le proprie partnership già utilizzate per la rete 4G con Huawei e Ericsson. Anche Yoigo (Grupo MásMóvil) prosegue la propria collaborazione con Ericsson, già fornitore dell'apparecchiatura 4G.

3.2.3 Francia

In Francia gli investimenti stranieri su asset strategici vengono regolati dall'articolo 151-3 del *Code monétaire et financier*. In particolare, la disposizione normativa prevede che siano soggetti all'autorizzazione preventiva del Ministro dell'Economia gli investimenti, anche su base occasionale, che possono interferire con l'esercizio dei poteri governativi o che rientrano in una delle seguenti aree:

- attività che potrebbero pregiudicare l'ordine pubblico, la sicurezza pubblica o gli interessi della difesa nazionale;
- attività di ricerca, produzione o commercializzazione di armi, munizioni, polveri e sostanze esplosive;
- in caso di investimenti di soggetti extra UE il campo di applicazione si amplia al gioco d'azzardo, alla sicurezza privata, alla crittografia nonché alla sicurezza dei sistemi informativi.

In questo scenario si inserisce la delicata discussione riguardo l'infrastrutturazione delle reti mobili di quinta generazione. Il Primo Ministro francese Macron, dopo un meeting con il Ministro degli Esteri francese, ha dichiarato che la Francia non escluderà Huawei dal suo network 5G, pur favorendo *vendor* europei tramite una limitazione ad otto anni delle licenze stipulabili con Huawei[53]. Per acquistare apparecchiature di fornitori extra-europei le telco dovranno richiedere l'autorizzazione del Governo, che si riserva la possibilità di valutare **caso per caso**. Guillaume Poupard, direttore generale dell'Agenzia nazionale della sicurezza dei sistemi di informazione

[53] https://www.reuters.com/article/us-france-macron-huawei/macron-says-frances-5g-strategy-founded-on-european-sovereignty-idUSKBN25O2IJ

(Anssi), ha espresso[54] la necessità di sviluppare il 5G in condizioni economiche accettabili per gli operatori di telecomunicazioni, senza essere dipendenti da nessun fornitore specifico.

Per gli operatori di rete che stanno già utilizzando apparecchiature di vendor extra-europei, la Francia ha deciso momentaneamente di concedere autorizzazioni per periodi che variano tra i tre e gli otto anni. La decisione del Governo francese sulle apparecchiature dei fornitori extra-europei risulta cruciale in particolar modo per Bouygues Telecom e SFR, due dei quattro operatori di telecomunicazioni del Paese, in quanto circa la metà della loro attuale rete mobile è affidata a fornitori asiatici. Nel dettaglio, per quel che concerne gli operatori di rete francesi, le operazioni relative alla stipula o al rinnovo degli accordi in vista della prossima fase di infrastrutturazione sono state rese più complesse. Orange, primo operatore del Paese, si è visto respingere la richiesta di autorizzazione per l'utilizzo del 5G RAN di Huawei da parte del Governo.

Per tali ragioni, ha deciso di siglare accordi con i suoi precedenti fornitori Ericsson e Nokia anche per il 5G[55]. In modo simile si sono mossi anche gli altri due principali attori del mercato, Bouygues Telecom e SFR. In particolare, Bouygues sta procedendo all'implementazione della componentistica 5G di Ericsson, e intende effettuare una graduale sostituzione di 3000 antenne Huawei entro il 2028 a causa delle preoccupazioni derivanti dalla possibilità di mancati rinnovi dopo le valutazioni caso per caso stabilite dal Governo nazionale. SFR ha invece rinnovato con Nokia per la parte di rete già realizzata in 4G dall'operatore svedese e intende fare lo stesso con Huawei, al netto della concessione delle autorizzazioni governative. Per agevolare la fornitura, lo scorso marzo 2020 Huawei ha annunciato l'intenzione di aprire il primo impianto di produzione di apparecchiature per il 5G fuori dalla Cina proprio sul territorio francese. Anche il quarto operatore francese, Free, ha confermato per il 5G il proprio partner commerciale utilizzato per il 4G, ovvero Nokia[56].

[54] https://www.lesechos.fr/tech-medias/hightech/il-ny-aura-pas-un-bannissement-total-de-huawei-affirme-le-patron-de-lanssi-1221434

[55] La partnership con Nokia è relativa alle regioni occidentali e sud orientali della Francia, in cui Nokia fornisce già le apparecchiature per le reti di accesso mobili (RAN) 2G/3G/4G. La partnership con Ericsson è relativa all'Ile de France ed alle regioni nord-orientali e sud-occidentali in cui Ericsson fornisce già apparecchiature per le reti di accesso mobili 2G/3G/4G.

[56] https://www.nokia.com/about-us/news/releases/2020/02/14/nokia-partners-with-iiiad-group-to-roll-out-5g-in-france-and-italy/

Lo stato di emergenza scatenato dalla pandemia di Covid-19 ha invece costretto l'Arcep, l'autorità di regolazione delle telecomunicazioni, a sospendere l'asta dello spettro 5G prevista per aprile 2020. Nella predisposizione del bando, l'Arcep ha deliberato che gli operatori di telecomunicazione francesi siano soggetti ad alcuni obblighi temporali, tra cui la copertura di almeno due città francesi entro il 2020. Gli operatori dovranno inoltre installare fino a 3.000 siti 5G entro il 2022, 8.000 entro il 2024 e 12.000 entro il 2025 nonché la copertura delle principali arterie stradali entro il 2027. I siti 5G sui corridoi di trasporto principali dovranno inoltre fornire una portata minima di 100 Mbps. L'asta, da cui si prevedeva un incasso di 2,2 miliardi di euro, è stata riaperta a settembre 2020 e si è conclusa il 1° Ottobre con l'assegnazione di 90 MHz a Orange (per 854 milioni); 80 MHz a SFR (per 728 milioni) e con 70 MHz a testa per Bouygues Telecom e Iliad (per 602 ciascuna), raggiungendo un totale di €2,8 miliardi

Attualmente nel mercato francese dei vendor di apparecchiature di rete 5G operano tre soggetti: due comunitari, Nokia e Ericsson, che insieme detengono il 75% della quota di mercato, e Huawei, di provenienza cinese. Per via di tale ristretto numero di fornitori, l'esclusione di uno dei già pochi rivenditori dal mercato potrebbe non solo limitare le possibilità di scelta da parte degli operatori telefonici, ma anche causare sensibili ritardi nell'infrastrutturazione della rete, rendendo difficile il rispetto del cronoprogramma dettato dall'Arcep.

3.2.4 Regno Unito

Il Regno Unito è **uno dei Paesi più all'avanguardia** nell'individuazione degli standard di sicurezza delle reti di telecomunicazioni. Dal 2010 il governo britannico ha istituito insieme a Huawei un centro indipendente di verifica dei prodotti del provider cinese, il Huawei Cyber Security Evaluation Centre (HC-SEC), all'interno del quale operano insieme dipendenti dell'azienda e personale dell'intelligence britannica. I servizi britannici, tramite un alto dirigente del Government Communications Headquarters (l'agenzia governativa che si occupa della sicurezza, spionaggio e controspionaggio), detengono la presidenza del HC-SEC.

A luglio 2020 il National Cyber Security Center (NCSC) ha disposto la **rimozione[57] di Huawei dalla rete 5G nazionale entro il 2027**, oltre ad un divieto sull'acquisto di nuove tecnologie del *vendor*

[57] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027#:~:text=There%20will%20be%20a%20ban,are%20manifested%20in%20the%20UK.

dopo il 31 dicembre 2020. Oltre a queste, le restrizioni esistenti sul *vendor* nelle infrastrutture strategiche rimangono comunque in atto. La decisione è tesa a migliorare sostanzialmente la sicurezza e la resilienza delle reti UK e si pone come conclusione della revisione della supply chain delle telecomunicazioni, pubblicata per la prima volta nel luglio 2019[58]. Sulla decisione si segnala anche la posizione della Commissione Difesa del parlamento britannico, la quale ha recentemente pubblicato un report[59] in cui si giustifica l'esclusione del provider cinese per via di atti collusivi con il Governo cinese.

Dal punto di vista economico, un report di Assembly[60] ha calcolato che una decisione di tale portata potrebbe determinare perdite fino a £18,2 miliardi. Nel rapporto si evidenzia anche come il divieto influenzerebbe l'attuale vantaggio competitivo del Regno Unito nella leadership sul 5G. Queste conclusioni si basano sulle stime, effettuate dallo stesso Governo britannico, relative ad un ritardo fino a 3 anni per l'implementazione della rete5G come conseguenza al divieto. Secondo il rapporto inoltre, la rimozione delle apparecchiature Huawei prima del 2027 porterebbe a un ulteriore ritardo nell'implementazione e a costi più elevati per l'economia del Regno Unito.

Negli ultimi 12 mesi, gli operatori di telefonia mobile del Regno Unito hanno compiuto progressi significativi nella distribuzione delle infrastrutture 5G, mettendo il Paese in una posizione forte per raccogliere i futuri benefici economici. Tuttavia, a causa della continua pressione degli Stati Uniti e delle ultime sanzioni, questo dispiegamento sembrerebbe destinato a rallentare, influenzando l'efficienza industriale, la competitività globale e i benefici economici associati all'essere un leader globale in 5G. Dei £18,2 miliardi di impatto economico, a causa del ritardo di 3 anni, circa £10 miliardi di benefici per la produttività andrebbero completamente persi. Inoltre, rispetto ad uno scenario in cui il Regno Unito figurava come uno dei leader globali nel campo del 5G, il declassamento dovuto a tale ritardo farebbe perdere al settore mobile l'opportunità di generare circa £4,7 miliardi, oltre circa £2 miliardi di benefici in meno generati dalle industrie correlate.

Il Ministro del Digital Matt Warman, in una dichiarazione datata settembre 2020, ha affermato[61] che la rimozione di Huawei dall'infrastruttura 5G del Regno Unito, pur fornendo nuove opportunità,

[58] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf
[59] https://publications.parliament.uk/pa/cm5801/cmselect/cmdfence/201/report-summary.html
[60] https://www.huawei.com/uk/news/uk/2020/assembly%20macroeconomic%20impact%20report
[61] https://www.5gradar.com/news/digital-minister-says-huaweis-5g-removal-is-a-big-hassle-factor-for-the-uk

causerà anche un "*grande fattore di fastidio*" per il governo, che dovrà anche evitare che l'ecosistema finale finisca per favorire un ridotto numero di *vendor*. Tuttavia, è stato anche stimato che un "reset" di questo tipo potrebbe favorire altri vendor che fino a questo momento non hanno avuto modo di competere per via degli accordi pluriennali già stipulati dagli operatori con i *competitor*[62].

Tra gli operatori, Vodafone e British Telecom (BT) hanno dichiarato che i propri consumatori potrebbero incorrere in problemi di connessione se non verrà fornito abbastanza tempo per la transizione annunciata[63]. Secondo fonti interne a Vodafone, per implementare la parte core della rete 5G senza la componentistica fornita dall'azienda cinese, la telco dovrà sostenere una spesa aggiuntiva di 200 milioni di sterline[64]. BT ha invece dichiarato che la decisione della Gran Bretagna di limitare il coinvolgimento di Huawei farà aumentare il costo del suo piano di sviluppo di circa 500 milioni di sterline. L'ingente esborso deriva dall'acquisto da parte dell'azienda di EE nel 2016, altro operatore di primo piano nel Paese, che ha realizzato l'intera infrastruttura 4G utilizzando apparecchiature Huawei e ha iniziato il *roll-out* del 5G con lo stesso *vendor*. Dopo quindici anni di collaborazioni con il colosso cinese, BT ha recentemente annunciato un accordo con Nokia per la realizzazione di nuove infrastrutture per il 5G in seguito alle decisioni del Governo britannico.[65]

3.2.5 Strategie di scelta del vendor da parte dei maggiori operatori europei

Analizzando le scelte degli operatori dei maggiori Paesi europei relative alla fornitura di apparecchiature di rete 5G, appare opportuno fare una serie di considerazioni. In primo luogo, per gli operatori di rete l'upgrade al 5G non può essere considerato come un *nice-to-have*. Infatti, nei limiti della disponibilità di frequenze per il nuovo standard, l'upgrade si configura come un ***must-have*** che nessun operatore, se vuole rimanere competitivo, può permettersi di non avere. In secondo luogo, osservando il trend e i risultati relativi alla sottoscrizione degli accordi a livello mondiale, emerge come il mercato si mantenga piuttosto **ristretto** e, con particolare riferimento all'Europa, la scelta sia confinata a tre operatori principali: Huawei, Ericsson e Nokia. In terzo luogo, si osserva come, in particolare nelle reti mobili, le posizioni di mercato siano direttamente collegate

[62] https://www.5gradar.com/features/the-5g-huawei-ban-short-term-pain-could-bring-long-term-gain
[63] https://www.bbc.com/news/technology-53349021
[64] Questa valutazione è stata rilasciata dal Ceo di Vodafone Nick Read alla conferenza stampa del Mobile World Congress di Barcellona 2019.
[65] https://www.zdnet.com/article/5g-bt-picks-nokia-to-power-networks-as-uk-starts-to-phases-out-huawei/

alla **compatibilità delle apparecchiature**: per evitare problemi di interoperabilità, un operatore che intenda cambiare fornitore per l'upgrade della rete al 5G dovrebbe aggiornare con le apparecchiature del nuovo fornitore anche la propria rete 4G già esistente. Il cambio di fornitore dovrebbe diventare più semplice con la variante *stand-alone* dello standard 5G, sebbene anche in questo caso i benefici derivanti dal mantenimento dello stesso fornitore rimangano molti. A conferma di ciò, la mappa degli accordi per il 5G degli operatori di rete dei maggiori Paesi europei mostra la generale **tendenza al rinnovo degli accordi** con il precedente fornitore, salvo che per due motivazioni principali: diversificazione della fornitura o ragioni regolamentari.

In Francia, Orange ha rinnovato anche per il 5G gli accordi con i propri precedenti fornitori 4G, Ericsson e Nokia. Sulla stessa lunghezza d'onda si sono mossi Bouygues Telecom e SFR, che hanno rinnovato gli accordi rispettivamente con Ericsson e Nokia e avevano espresso la volontà di fare lo stesso con Huawei, salvo l'ottenimento dei permessi da parte del Governo. Anche il quarto operatore francese, Free, ha confermato per il 5G il proprio partner commerciale utilizzato per il 4G, ovvero Nokia.

In Germania, al netto di eventuali disposizioni normative attese nelle prossime settimane, tutti e tre gli operatori avevano rinnovato o erano in procinto di rinnovare gli stessi accordi *multi-vendor* con i fornitori già attivi sulla rete 4G: Ericsson/Huawei per Deutsche Telekom (sebbene la chiusura degli accordi sia in attesa delle decisioni politiche), Nokia/Huawei per Telefónica Germany (che punterà maggiormente sulla diversificazione anche della rete core dal 2024) ed Ericsson/Huawei per Vodafone.

Un discorso simile può essere fatto per la Spagna, dove Vodafone España ha rinnovato con Ericsson e Huawei (già fornitori 4G); Orange Espagne ha rinnovato gli accordi con Ericsson e Huawei allargando la propria schiera di fornitori 5G anche a ZTE; e Telefónica (Movistar) ha rinnovato con Ericsson e Nokia e allargato la fornitura 5G anche Huawei.

Anche in Gran Bretagna, dove la normativa punta all'esclusione di Huawei per il 2028, si osserva un rinnovo multi-vendor con gli stessi operatori già fornitori nel 4G, ovvero Nokia e Huawei per 3 – Three; Ericsson e Nokia per Telefónica (O2); e Ericsson e Huawei sia per BT Group (EE), sia per Vodafone.
Un discorso simile vale anche per l'Italia, dove al momento si osservano prevalentemente rinnovi multi-vendor con gli stessi fornitori del 4G.

In definitiva, dunque, si osserva come questi tre fattori, ovvero mercato dell'offerta di apparecchiature 5G ristretto a 3-4 fornitori, necessità di compatibilità tra apparecchiature (e quindi fornitori) 4G e 5G, ed evoluzione delle normative tendente ad un'ulteriore restrizione del mercato dell'offerta per ragioni geopolitiche, determinino una situazione di stallo o rallentamento nelle operazioni di infrastrutturazione che rischia di avere a sua volta effettivi negativi in termini di minore sviluppo tecnologico e ritardati (e probabilmente anche minori) benefici economici derivanti dalla rivoluzione 5G.

TABELLA 3.1 Accordi di fornitura 5G tra operatori e vendor nei maggiori Paesi europei

Stato	Operatore	Vendor 4G	Vendor 5G	Info aggiuntive
Francia	Bouygues Telecom	Ericsson/Huawei	Ericsson + in talks with Huawei	L'operatore sta procedendo all'implementazione della componentistica 5G di Ericsson e intende effettuare l'upgrade sulle parti 4G della rete di Huawei con le apparecchiature del fornitore cinese, che dipenderà dalla valutazione del Governo francese
	Free Mobile	Nokia	Nokia	
	Orange	Ericsson/Nokia	Ericsson/Nokia	Rinnovate le partnership per le diverse regioni del Paese già coperte in 4G.
	SFR	Nokia/Huawei	Nokia + in talks with Huawei	Upgrade della rete esistente di Nokia con apparecchiature 5G dello stesso operatore e intenzione di effettuare l'upgrade della parte delle 4G fornita da Huawei con le apparecchiature del fornitore cinese. Anche in questo caso è necessario l'ok del Governo francese.
Germania	Deutsche Telekom (T-Mobile)	Ericsson/Huawei	Ericsson/Huawei	L'accordo con Ericsson è stato rinnovato, mentre quello con Huawei è in stand-by, in attesa delle eventuali evoluzioni normative
	Telefónica Germany (O2)	Nokia/Huawei	Nokia/Huawei	Entro il 2024 intendono cessare la partecipazione con Huawei nella rete core per ragioni tecniche relative alla diversificazione
	Vodafone	Ericsson/Huawei	Ericsson/Huawei	Al netto di eventuali limitazioni dovute all'aggiornamento della normativa

Spagna	Orange Espagne	Ericsson/Huawei	Ericsson/Huawei/ZTE	Huawei ha il 50% del network, Ericsson il 45% e ZTE il 5%, con quest'ultimo in sensibile crescita.
	Telefónica (Movistar)	Ericsson/Nokia	Ericsson/Nokia /Huawei	Entro il 2024 intendono cambiare fornitore di rete core per ragioni tecniche relative alla diversificazione
	Vodafone España	Ericsson/Huawei	Ericsson/Huawei	
	Yoigo	Ericsson	Ericsson	
Regno Unito	3 - Three	Nokia/Huawei	Nokia/Huawei	Era prevista la partecipazione di Huawei nella rete di accesso con cap al 35% del totale. Il successivo aggiornamento normativo prevede la rimozione di Huawei entro il 2027, e il divieto di acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020.
	BT Group (EE)	Ericsson/Huawei	Ericsson/Huawei	Era prevista la partecipazione di Huawei nella rete di accesso con cap al 35% del totale. Il successivo aggiornamento normativo prevede la rimozione di Huawei entro il 2027, e il divieto di acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020.
	Telefónica (O2)	Ericsson/Nokia	Ericsson/Nokia	Era prevista la partecipazione di Huawei nella rete di accesso con cap al 35% del totale. Il successivo aggiornamento normativo prevede la rimozione di Huawei entro il 2027, e il divieto di acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020.
	Vodafone	Ericsson/Huawei	Ericsson/Huawei	Entro il 2025 intendeva limitare la fornitura di Huawei alla rete di accesso, mantenendo la sua percentuale entro il 35% del totale. Il successivo aggiornamento normativo prevede la rimozione di Huawei entro il 2027, e il divieto di acquisto di nuove tecnologie del vendor dopo il 31 dicembre 2020.
Italia	Iliad	Nokia	Nokia	

	TIM	Ericsson/Nokia/Huawei	Ericsson/ Nokia/ Huawei	Da confermare
	Vodafone Italia	Huawei/Nokia	Huawei/Nokia	
	Wind Tre	ZTE/Ericsson	ZTE/Ericsson	

Fonte: Elaborazioni I-Com su varie

4. L'ITALIA A 5G

4.1. STATO DELL'ARTE E PROSPETTIVE FUTURE (DESI, SPERIMENTAZIONI, INDAGINE CONOSCITIVA, OSTACOLI DI VARIA NATURA)

Se in Asia e negli Usa la diffusione del 5G sta mostrando costanti progressi, in Italia il buon posizionamento che era stato registrato anche dalle statistiche internazionali sembra essere complicato da una serie di fattori, tra cui il **rallentamento delle opere di infrastrutturazione per via del Covid**, la crescente paura della popolazione generata dalla diffusione di *fake news* sulla sua presenta pericolosità (a sua volta cavalcata da alcune amministrazioni locali a fini elettorali), ed al rischio di riduzione degli investimenti dovuta, oltre che alle alte licenze pagate, anche alla contrazione dei ricavi del settore.

Tra le note positive c'è senza dubbio il posizionamento nella classifica del DESI, che vede l'Italia ancora in terza posizione, dopo il secondo posto registrato nel 2019. Andando nel dettaglio, tuttavia, si osserva come tale indicatore sia composto sostanzialmente dalle percentuali di assegnazione delle 3 bande di frequenze. La seconda posizione è stata quindi garantita dal grande scatto in avanti effettuato mettendo a gara tutte e tre le frequenze già nel 2018, una mossa che ci ha visto primi in Europa e secondi nel mondo in termini di assegnazione della banda a 26 GHz. Peraltro, la banda a 700 Mhz è stata assegnata con riserva, quindi pagata (o messa a bilancio) dagli operatori ma non disponibile per sperimentazioni e offerta di servizi fino a giugno 2022. Per tali ragioni, rispetto all'indicatore 5G readiness del Desi, l'Italia non ha più terreno da guadagnare, salvo quando le licenze per la banda a 700Mhz verranno effettivamente assegnate agli operatori.

Un secondo parametro che viene considerato a livello europeo riguarda le **sperimentazioni di servizi**, censite in particolare dal 5G Observatory. A settembre 2020, l'Osservatorio ne ha registrate 21 effettuate in Italia, che collocano il nostro Paese in terza posizione dietro a Spagna (31) e Germania (22), seguita da Francia (19) e Regno Unito (18). Tuttavia, altri due parametri risultano interessanti per comprendere lo stato di sviluppo e le prospettive del 5G, ovvero il livello di complessità delle sperimentazioni e la loro evoluzione temporale. Per quanto concerne il primo aspetto, il 5G Observatory ha classificato le maggiori sperimentazioni in Europa e Paesi limitrofi distinguendo tra tre categorie: (1) progetti pilota più importanti, ovvero che coinvolgono almeno due siti (*small cell*) e gli utenti finali; (2) altri progetti; e (3) test minori e/o dimostrazioni. Applicando tali criteri ai 5 maggiori Paesi europei si nota, in primo luogo, come gran parte della sperimentazioni sia classificabile nella categoria inferiore; in secondo luogo, si osserva come l'Italia sia posizionata meno bene di come si potrebbe pensare (Tab. 4.1), con solo due progetti di maggiore entità

all'attivo (nel dettaglio quelli condotti da Tim con Ericsson and Qualcomm), e 6 progetti intermedi (a Milano, Torino, Roma, Cagliari e Genova).

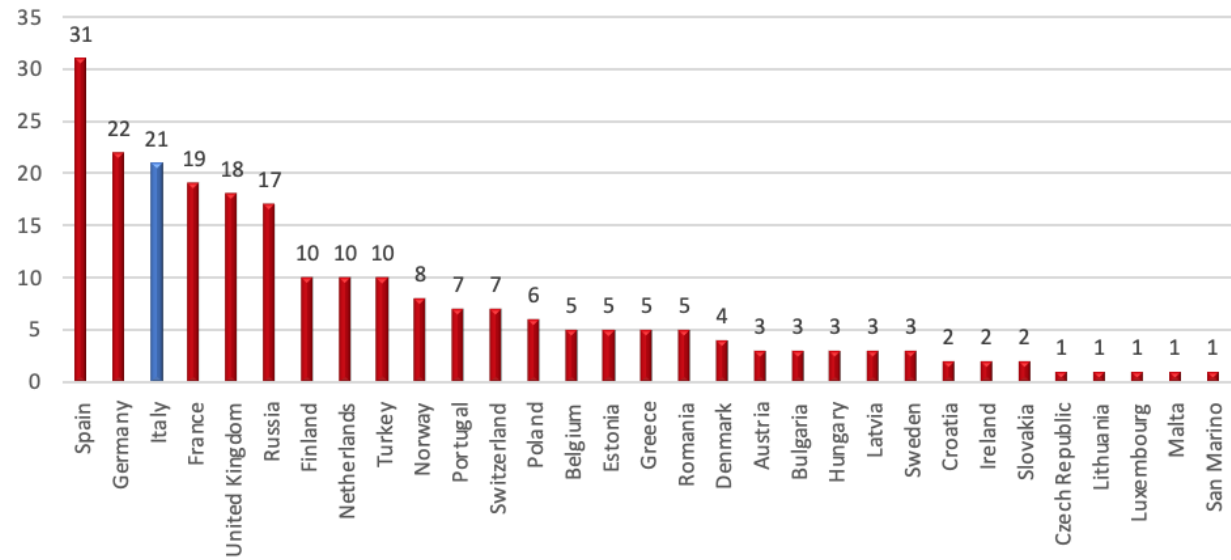

FIGURA 4.1 Sperimentazioni 5G in Italia e in Europa (settembre 2020)

Fonte: 5G Observatory

TABELLA 4.1 Sperimentazioni nei maggiori Paesi europei per livello di maturità (settembre 2020)

Paese	Conteggio di Level of maturity*			Totale Paese
	1	2	3	
Spain	5	9	17	31
United Kingdom	4	3	11	18
Germany	3	9	10	22
Italy	2	6	13	21
France	2	4	13	19
Totale per livello di maturità	16	31	64	111

* con il livello [1] vengono indentificati i progetti più importanti (2 cell sites); con livello [2] gli altri progetti pilota; con il livello [3] le sperimentazioni minori

Fonte: 5G Observatory

L'evoluzione del numero delle sperimentazioni nel tempo, inoltre, sembra mostrare un andamento che ha raggiunto il proprio apice nel 2018, anno in cui nei principali Paesi europei si sono registrati 42 casi, mentre dal 2019 sembra si sia avviato un leggero declino, trasformatosi in un vero e proprio calo nel 2020, evidentemente dovuta anche all'emergenza sanitaria. Secondo il 5G Observatory, da giungo 2020 sono stati registrate soltanto 2 sperimentazioni in Europa, rispettivamente in Germania (Deutsche Telekom a Düsseldorf) e Malta (Melita), cui va aggiunta quella più recente di TIM, che ha stabilito un nuovo record di velocità (4 Gigabit al secondo in *downlink*) nella banda a 26 Ghz in collaborazione con Qualcomm ed Ericsson.

TABELLA 4.2 Sperimentazioni nei maggiori Paesi europei 2015-2020 (settembre 2020)

	2015	2016	2017	2018	2019	2020	Totale Paese
Spain	1	3	6	11	7	3	31
Germany	1	5	4	6	4	2	22
Italy	0	3	4	9	3	2	21
France	0	1	5	11	2	0	19
United Kingdom	0	4	4	5	5	0	18
Totale per anno	2	16	23	42	21	7	111

Fonte: 5G Observatory

Tale rallentamento potrebbe anche essere sintomo del fatto che la tecnologia non è matura per supportare il lancio di servizi avanzati. In Italia, allo stato attuale, gli operatori stanno procedendo alla graduale **installazione di antenne ed al lancio dei servizi di connettività** di nuova generazione. Servizi commerciali 5G sono stati già lanciati da Tim e Vodafone, in modalità business e consumer, a Roma, Milano, Torino, Firenze, Napoli, Bologna, Genova, Sanremo, Brescia e Monza. Inoltre, Vodafone ha già esteso la propria rete anche a gran parte dell'hinterland milanese, mentre Tim ne ha avviato la fase di sperimentazione nella Repubblica di San Marino, a Bari e a Matera dove, con i fondi aggiudicati dal primo bando di gara del MiSE, si sta realizzando il progetto BariMatera5G.

Tim e Vodafone hanno anche siglato un accordo per la creazione di una rete condivisa, grazie alla quale, entro il 2021, dovrebbero essere coperte in 5G altre 100 città italiane, oltre a numerosi distretti industriali e alle principali località turistiche. Anche WindTre sta procedendo all'installazione di antenne proprie, ed il servizio per gli abbonati dovrebbe essere disponibile nelle

principali città italiane entro la fine del 2020 ed in 70 città entro il 2021. Negli ultimi mesi anche Iliad ha iniziato a ottenere le autorizzazioni necessarie per l'installazione di antenne 5G in vari impianti del territorio nazionale, facendo affidamento su apparati forniti da Nokia, come già avvenuto in Francia.

Relativamente agli investimenti necessari per sviluppare la rete 5G in Italia, nel 2018, Asstel[66] ha effettuato la seguente stima: nel dettaglio, vengono indicate due forchette di costo relative in primo luogo gli investimenti *as usual*, che vanno dagli € 35 ai 45 miliardi, ed in secondo luogo per la posa di ulteriore fibra e delle reti 5G, stimati tra gli € 15 ai 20 miliardi, per un totale che, considerando anche i costi per le licenze, ammonterebbe ad un cifra compresa tra i € 55 e i 70 miliardi. Sulla base di tali dati, EY ha effettuato un'ulteriore stima degli investimenti necessari all'implementazione delle reti 5G anche alla luce di possibili restrizioni verso *vendor* extra-europei. Nel complesso, EY valuta l'impatto economico delle eventuali restrizioni in una forchetta compresa tra i €4 e 5 miliardi aggiuntivi, in termini di costi per gli operatori per la sostituzione e l'upgrade degli apparecchi con nuovi dispositivi forniti da operatori europei, insieme ad un ritardo di circa 18 mesi nella diffusione di copertura e servizi.

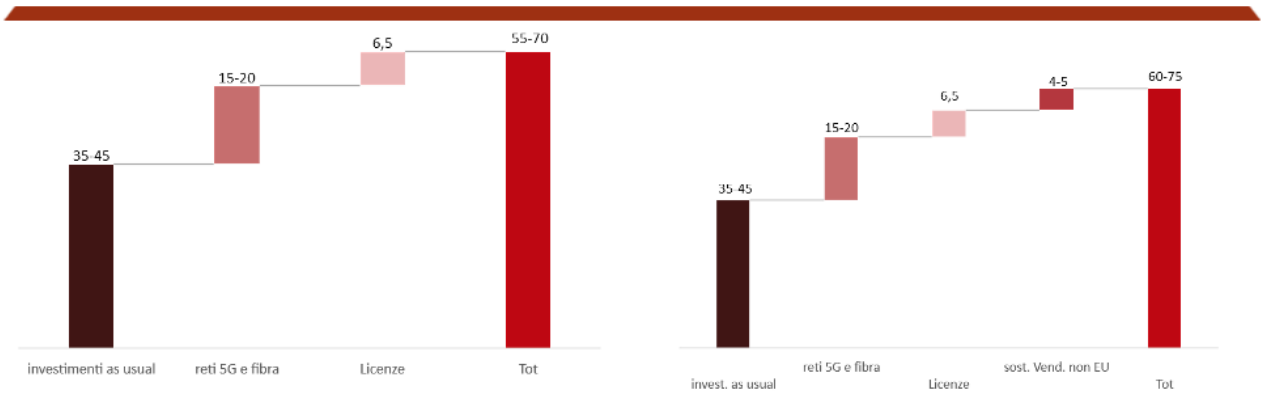

FIGURA 4.2 Stima investimenti necessari per l'implementazione delle reti 5G in Italia (in € mld, 2019-2025)

Fonte: Elaborazioni I-Com su dati Asstel, EY e Commissione Europea, 2020

A tal proposito, è possibile comparare tale fabbisogno stimato con gli **investimenti in infrastrutture** rilevati da Agcom. Questi ultimi risultano nel complesso relativamente stabili nella rete fissa,

[66] Assotelecomunicazioni-Asstel ha presentato questi dati nel corso dell'audizione alla Camera che si è svolta ad aprile 2019 in materia di 5G, Big Data ed elettromagnetismo.

mentre presentano una flessione nella rete mobile, dovuta, secondo l'Authority, al venir meno dei fondi investiti dalle imprese per sostenere le aggiudicazioni delle licenze nella gara per le frequenze 5G.

TABELLA 4.3 Investimenti in immobilizzazione su rete fissa e mobile (€ miliardi, 2015-2019)

	2015	2016	2017	2018	2019	tot 2015-2019
Mobile	3,11	2,47	2,3	3,14	2,73	13,75
Fissa	4,18	4,58	4,88	5,16	5,14	23,94
Totale	7,29	7,04	7,18	8,3	7,87	37,68

Fonte: 5G Observatory

Nel complesso, nell'ultimo quinquennio sono stati investiti nelle reti mobili circa €13,7 miliardi, ovvero meno del 20% di quanto occorrebbe investire nei prossimi 5 anni nel caso dello scenario più costoso (€75 miliardi) e circa il 25% di quanto occorrebbe nello scenario migliore (€55 miliardi). In altre parole, gli operatori di rete nei prossimi 5 anni potrebbero dover incrementare i propri investimenti fino a 5 volte, rispetto a quanto avvenuto nell'ultimo quinquennio.

Alla luce di tali considerazioni, appare evidente la necessità di andare a snellire le procedure ed i vincoli burocratici per incentivare gli operatori a incrementare e velocizzare i propri investimenti nelle reti mobili, in particolare favorendo la diffusione del nuovo standard 5G. Come osservato nel cap. 1, nel corso delle audizioni al Senato in vista del recepimento del Codice europeo delle comunicazioni elettroniche, i principali operatori di rete hanno espresso le proprie perplessità riguardo gli eccessivi vincoli burocratici che stanno rallentando l'iter di ottenimento delle autorizzazioni per investire sulle infrastrutture 5G. Tra le diverse criticità evidenziate si annoverano la necessità di attuare nel più breve tempo possibile la legge sul perimetro di sicurezza nazionale cibernetica (cfr. par. 4.2), l'importanza di uniformare la normativa italiana sulle emissioni a quella dell'Unione Europea e semplificare le norme che regolano interventi e installazioni, non sempre omogenee su tutto il territorio nazionale, al fine di evitare l'insorgere di gap tecnologici tra un'area e l'altra del Paese.

Per quanto concerne i **limiti elettromagnetici**, come noto l'Italia presenta i vincoli più stringenti, in termini di potenza erogabile, rispetto a tutti gli altri Paesi europei. Nel dettaglio, il limite consentito

ammonta a circa un decimo rispetto a quello consigliato dall'ICNIRP[67]. Inoltre la normativa non distingue tra le diverse bande di frequenza ed il limite viene ulteriormente abbassato[68] poiché questa è la soglia consentita nelle zone in cui si registra la permanenza delle persone per più di 4 ore. Per il 5G, le criticità relative alla mancata differenziazione tra le diverse bande emergono in particolare in relazione alla porzione 3.4-3.8 GHz (la banda pioniera identificata per le sperimentazioni), per la quale da anni viene consigliato il limite di 61 V/m, che in Italia è di 10 volte inferiore: 6 V/m.

D'altro canto, la regolazione dei limiti elettromagnetici così basso, se da un lato potrebbe conferire un maggiore grado di sicurezza ai cittadini, dall'altro comporta alcune controindicazioni a livello di copertura e di qualità dei servizi relative alle comunicazioni senza fili. Ciò è dovuto, in primo luogo, al fatto che limiti più bassi richiedono l'installazione di un numero maggiore di impianti, limitando inoltre la capacità di copertura in particolare relativa agli interni di abitazioni, fabbriche e uffici. Per quanto concerne il 5G, in particolare, le restrizioni non consentono di utilizzare tutti i siti di cui gli operatori potrebbero disporre per posizionare le infrastrutture di rete quali impianti e antenne.

A tal proposito, il Politecnico di Milano[69] ha effettuato una comparazione tra agli impianti necessari a coprire il territorio con i limiti consigliati da ICNIRP e quelli stabiliti in Italia: se con i primi

[67] A livello ambientale, i limiti sono calcolati in volt per metro (V/m, che misura l'intensità del campo elettromagnetico) ed in Watt per metro quadro (W/m2, che indica l'uso della densità di potenza). Il valore consigliato è equivalente a 61V/m, pari a 10 W/m2. In Italia la normativa ha ridotto in maniera sensibile tali limiti, assestandoli a 6 V/m, pari a 0,1 W/m2. Tale disciplina è stata approvata nel 2001 (legge n.36) e poi integrata nel 2003 e nel 2012.

[68] Il limite, stabilito in 20 V/m, di fatto viene abbassato a 6 V/m in tutte quelle urbanizzate o semi urbanizzate.

[69] Il Politecnico di Milano ha condotto uno studio per conto di Asstel ed in collaborazione con gli operatori di rete mobile volto ad analizzare i possibili scenari di sviluppo delle reti 5G in relazione ai limiti elettromagnetici (2018). L'analisi è stata condotta limitatamente allo spettro di frequenze 3.6-3.8 GHz e si basa su stime "informate" e ipotesi "di scuola" definite dal Politecnico sulla base di informazioni ricevute singolarmente dagli Operatori. Sono state analizzate 5 città campione ritenute significative (Torino, Modena, Trieste, Caserta, Rimini) e si è poi proceduto ad estrapolare i dati a livello nazionale ipotizzando di utilizzare primariamente le infrastrutture preesistenti ove i limiti lo permettessero. Per la definizione degli interventi necessari allo sviluppo della rete 5G sul territorio nazionale sono stati considerati i vincoli imposti alle infrastrutture di reti radiomobili. Per i costi, sono state usate delle stime relative ai costi di investimento (CAPEX) ed ai costi di esercizio (OPEX), definite dal Politecnico di Milano sulla base delle informazioni ricevute singolarmente dagli Operatori, che sono state ritenute rappresentare una ragionevole simulazione della pianificazione per la costruzione delle reti 5G. Le stime riportate sono il risultato dell'esercizio di pianificazione su cui si basa lo studio. Esse non possono essere considerate stime dettagliate di costi per gli Operatori per il periodo di 10 anni per la quali sono state calcolate, perché su un periodo così lungo hanno impatto strategie di sviluppo e cambiamenti tecnologici che sono ovviamente imprevedibili ed estranei allo studio effettuato.

sembrerebbe possibile effettuare l'*upgrade* al 5G di tutti i siti già esistenti, lasciando quindi un numero di ulteriori siti da implementare che risulta così esiguo da risultare trascurabile, con i limiti più bassi attualmente previsti in Italia sembrerebbe possibile utilizzare soltanto il 48% dei siti già presenti, mentre una porzione equivalente a circa 27.000 unità (equivalente al 62% dei siti di trasmissione presenti in Italia) richiederebbero interventi o la predisposizione di siti da identificare

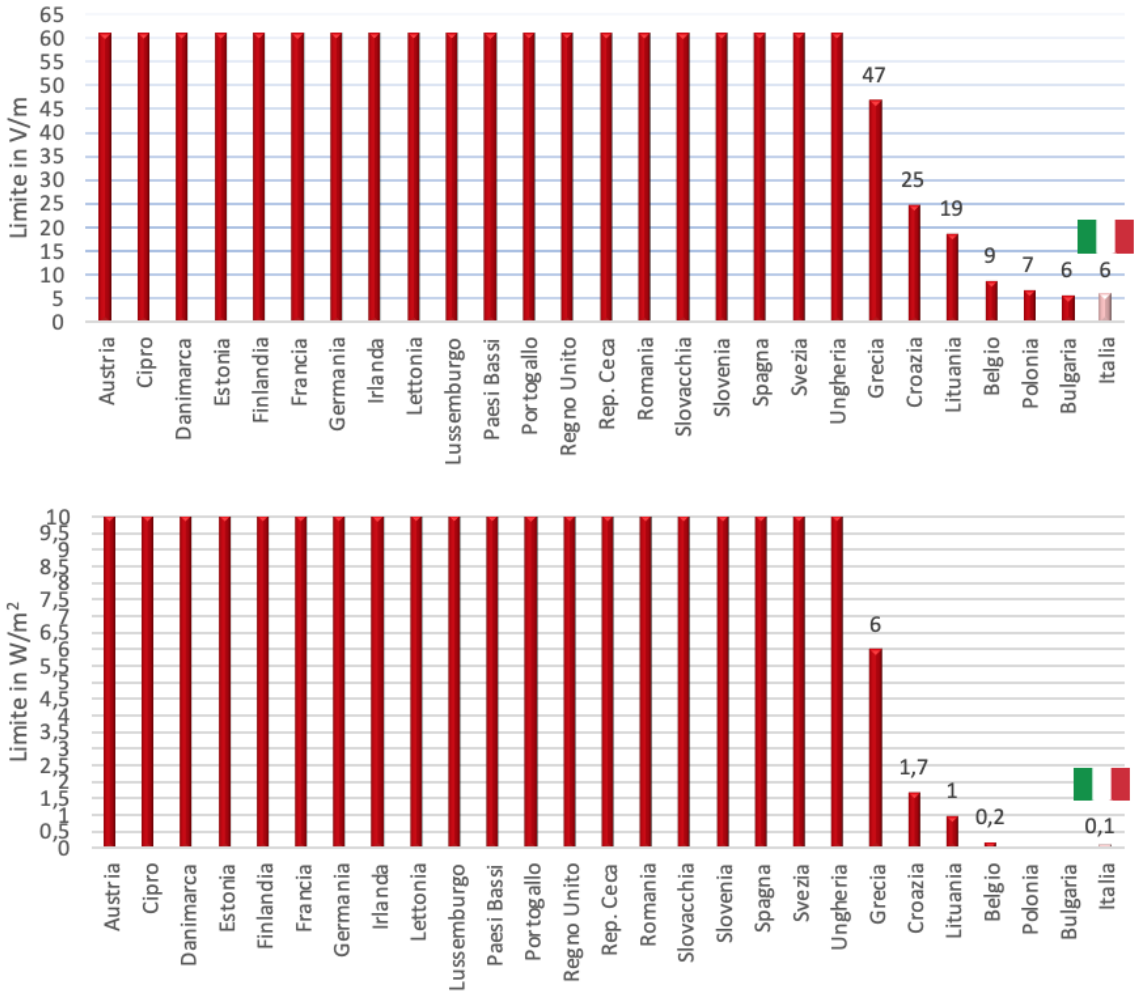

FIGURA 4.3 Limiti elettromagnetici in termini di V/m e W/m² : Italia vs altri Paesi europei

Fonte: National Institute for Public Health and the Environment, RIVM, Ministry of Health, Welfare e Sport, The Netherlands (novembre 2019)

ex-novo. Tale reingegnerizzazione della rete, oltre ai problemi di impatto regolamentare e paesaggistico che incontrerebbe per la necessità di trovare un numero così elevato di nuovi siti

adatti alla trasmissione, genererebbe extra costi fino a €3,9 miliardi, rispetto agli investimenti necessari ad ammodernare la rete che sarebbero necessari qualora i limiti elettromagnetici fossero equiparati a quelli consigliati dall'ICNIRP.

Al contrario, molteplici amministrazioni locali **hanno assecondato gli infondati timori** sui possibili rischi legati alla diffusione delle antenne 5G ed i relativi campi magnetici, approvando provvedimenti a livello locale per bloccarne la diffusione nei propri territori. A tal proposito, il **Decreto Semplificazioni** del 16 luglio 2020 è intervenuto sulle ordinanze pubblicate a livello comunale, lasciando ai sindaci la possibilità di adottare regole che minimizzino l'impatto per i propri cittadini, ma non consentendo loro di opporsi all'installazione delle antenne se queste rispettano i limiti di emissione dei campi elettromagnetici e i piani urbanistici.

4.2. L'APPROCCIO ITALIANO ALLA SICUREZZA DELLE RETI

4.2.1 Il recepimento della direttiva NIS in Italia e le iniziative a tutela della sicurezza delle reti

Il tema della sicurezza rappresenta una priorità anche per l'Italia. Dopo l'adozione, nel 2017, di alcuni provvedimenti propedeutici o preparatori all'adozione delle misure prescritte dalla direttiva NIS quali il Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" (il cosiddetto "DPCM Gentiloni"), che ha tra l'altro riorganizzato l'architettura per la protezione dello spazio cibernetico nazionale, ed il nuovo "Piano nazionale per la protezione cibernetica e la sicurezza informatica" (marzo 2017), che ha aggiornato gli indirizzi e le direttive stabilite col precedente Piano del 2013 proprio in vista delle indicazioni presenti nella direttiva NIS, con il **D.Lgs. n. 65 del 18 maggio 2018** l'Italia ha recepito la direttiva NIS. Si tratta di un intervento importante, sebbene non particolarmente innovativo nella sostanza rispetto a quanto previsto dalla direttiva NIS, che istituisce un elenco nazionale degli operatori di servizi essenziali presso il MiSE, individua (all'art. 5) gli elementi da considerare ai fini della determinazione della rilevanza degli effetti negativi, declina i contenuti della strategia nazionale, ripartisce le competenze tra 5 Ministeri (Sviluppo economico, Infrastrutture e trasporti, Economia, Salute e Ambiente) (art. 7) – incaricando il Dipartimento delle informazioni per la sicurezza (DIS) di svolgere le funzioni di punto di contatto unico e istituendo, presso la Presidenza del Consiglio dei Ministri, un unico Computer Security Incident Response Team, detto CSIRT italiano – ripropone gli specifici obblighi in materia di

sicurezza gravanti sugli operatori di servizi essenziali, prescrive obblighi di notifica al CSIRT per gli operatori di servizi essenziali e per i fornitori di servizi digitali inoltrino al CSIRT e declina un set di sanzioni in relazione alle diverse possibili infrazioni che possono essere poste in essere dagli operatori di servizi essenziali e dai fornitori di servizi digitali, fino ad un massimo di € 150.000.

Quanto al CSIRT, cui spettano importantissime funzioni tra cui la definizione delle procedure per la prevenzione e la gestione dei *cyber incidents* e la ricezione delle segnalazioni di incidente, è di maggio l'ufficiale accorpamento del Computer Security Incident Response Team nel Dipartimento delle Informazioni per la Sicurezza (DIS). Cruciale sarà l'attenzione agli asset, il loro utilizzo e la loro vulnerabilità, soprattutto con riguardo al 5G. Ciò comporterà, con schede e segnalazioni studiate *ad hoc*, la possibilità di minimizzare i rischi di tutti i sistemi informativi, sistemi informatici e di associare rapidamente l'approvvigionamento di prodotti e dei processi alle infrastrutture scongiurando il c.d. rischio sistemico. Il DIS, perciò, sarà fondamentale per l'analisi dei fenomeni strategici e sociali nei settori della difesa e della sicurezza nazionale.

Se questo, sinteticamente, è il quadro generale, l'Italia, come l'Europa, si trova a fronteggiare un'altra sfida cruciale per il futuro del sistema paese: garantire la sicurezza delle reti 5G. Per analizzare le iniziative intraprese a livello nazionale a tal fine, è necessario, preliminarmente, ripercorrere sinteticamente la storia dell'introduzione in Italia della disciplina relativa alla golden share, poi golden power. La *golden share*, in particolare, è propria della tradizione britannica e fa riferimento alla conservazione, da parte dello Stato, nell'ambito di procedure di privatizzazione di imprese in origine pubbliche, di una partecipazione azionaria con poteri esorbitanti rispetto a quelli spettanti ad un normale azionista.

Si tratta di uno strumento che è stato introdotto nel nostro ordinamento con il **decreto legge 31 maggio 1994, n. 332, convertito con legge 30 luglio 1994, n. 474** e rivisto, a seguito della Comunicazione n. C220 del 19/07/1997 della Corte di Giustizia – con la quale è stato precisato che l'esercizio di tali poteri deve comunque essere attuato senza discriminazioni, essere fondato su "*criteri obiettivi, stabili e resi pubblici*" ed essere giustificato da "*motivi imperiosi di interesse generale*" – con il **decreto legge 15 marzo 2012 n. 21, convertito con modificazioni con la legge n. 56 del 2012.** Tale decreto ha ridisegnato il quadro normativo segnando il passaggio dalla *golden share* al c.d. "***golden power***", locuzione con cui si fa riferimento ad una serie di poteri esercitabili nei settori della difesa e della sicurezza nazionale, nonché in alcuni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.

La principale differenza con la normativa precedente, che segna, appunto, il passaggio dalla *golden share* al *golden power*, risiede nell'ambito operativo della nuova disciplina che, superando il precedente sistema che limitava l'esercizio dei poteri speciali alle società privatizzate o in mano pubblica, abilita l'esercizio di tali poteri speciali rispetto a tutte le società, sia pubbliche che private, che svolgono attività considerate di rilevanza strategica. Le norme affidano ad uno o più decreti del Presidente del Consiglio l'individuazione di attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale in rapporto alle quali potranno essere attivati i poteri speciali, l'individuazione della tipologia di atti o operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina, la concreta disciplina relativa all'esercizio dei poteri speciali nonché la previsione di ulteriori disposizioni attuative.

Con riferimento all'esercizio dei poteri speciali nei comparti della sicurezza e della difesa la normativa esige la sussistenza di una **minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale**. In tali ipotesi, al Governo è consentito: imporre specifiche condizioni all'acquisto di partecipazioni in imprese strategiche nel settore della difesa e della sicurezza; porre il veto all'adozione di delibere relative ad operazioni straordinarie o di particolare rilevanza, ivi incluse le modifiche di clausole statutarie eventualmente adottate in materia di limiti al diritto di voto o al possesso azionario; opporsi all'acquisto di partecipazioni, ove l'acquirente arrivi a detenere un livello della partecipazione al capitale in grado di compromettere gli interessi della difesa e della sicurezza nazionale.

Al fine di valutare la minaccia di grave pregiudizio agli interessi essenziali della difesa e della sicurezza nazionale, il Governo considera, tenendo conto dell'oggetto della delibera, la rilevanza strategica dei beni o delle imprese oggetto di trasferimento, l'idoneità dell'assetto risultante dalla delibera o dall'operazione a garantire l'integrità del sistema di difesa e sicurezza nazionale, la sicurezza delle informazioni relative alla difesa militare, gli interessi internazionali dello Stato, la protezione del territorio nazionale, delle infrastrutture critiche e strategiche e delle frontiere, nonché gli elementi di cui al comma 3 e, nello specifico: a) l'adeguatezza, tenuto conto anche delle modalità di finanziamento dell'acquisizione, della capacità economica, finanziaria, tecnica e organizzativa dell'acquirente nonché del progetto industriale, rispetto alla regolare prosecuzione delle attività, al mantenimento del patrimonio tecnologico, anche con riferimento alle attività strategiche chiave, alla sicurezza e alla continuità degli approvvigionamenti, oltre che alla corretta e puntuale esecuzione degli obblighi contrattuali assunti nei confronti di pubbliche

amministrazioni, direttamente o indirettamente, dalla società le cui partecipazioni sono oggetto di acquisizione, con specifico riguardo ai rapporti relativi alla difesa nazionale, all'ordine pubblico e alla sicurezza nazionale; b) l'esistenza, tenuto conto anche delle posizioni ufficiali dell'Unione Europea, di motivi oggettivi che facciano ritenere possibile la sussistenza di legami fra l'acquirente e Paesi terzi che non riconoscono i principi di democrazia o dello stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale, desunti dalla natura delle loro alleanze, o hanno rapporti con organizzazioni criminali o terroristiche o con soggetti ad esse comunque collegati.

Dal punto di vista procedurale, il decreto legge ha disciplinato puntualmente **termini e procedure da osservare**; il comma 4, in particolare, prescrive che ai fini dell'esercizio del potere di veto, l'impresa notifichi alla Presidenza del Consiglio dei Ministri una informativa completa sulla delibera o sull'atto da adottare in modo da consentire il tempestivo esercizio del potere di veto. Quest'ultimo, in particolare, deve essere comunicato dal Presidente del Consiglio entro 15 gg dalla notifica con possibilità, qualora si renda necessario richiedere informazioni all'impresa, di sospendere tale termine, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Le richieste di informazioni successive alla prima, invece, non sospendono i termini. Una volta decorsi i predetti termini, l'operazione oggetto di notifica può essere effettuata. Dalla violazione di tale disciplina la normativa fa discendere la nullità delle delibere o degli atti adottati, la facoltà, per il Governo, di ingiungere alla società ed all'eventuale controparte di ripristinare a proprie spese la situazione anteriore, nonché l'imposizione di una sanzione amministrativa pecuniaria fino al doppio del valore dell'operazione e comunque non inferiore all'uno per cento del fatturato cumulato realizzato dalle imprese coinvolte nell'ultimo esercizio per il quale sia stato approvato il bilancio.

L'art. 2 del decreto in esame ha invece affidato a regolamenti (anziché DPCM) da adottare, previo parere delle Commissioni parlamentari competenti, l'individuazione degli asset strategici nel settore dell'energia, dei trasporti e delle comunicazioni, l'esercizio dei poteri speciali e l'individuazione di ulteriori disposizioni attuative della nuova disciplina. I poteri speciali esercitabili nel settore dell'energia, dei trasporti e delle comunicazioni si sostanziano nella possibilità di far valere il veto dell'esecutivo alle delibere, agli atti e alle operazioni concernenti asset strategici, in presenza dei requisiti richiesti dalla legge, ovvero imporvi specifiche condizioni; di porre condizioni all'efficacia dell'acquisto di partecipazioni da parte di soggetti esterni all'UE in società che detengono attivi "strategici" e, in casi eccezionali, opporsi all'acquisto stesso. Gli obblighi di notifica

sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa – nazionale ed europea – di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, ivi compresi le reti e gli impianti necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali. Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Anche in tal caso, dalle violazioni delle previsioni appena descritte discende la sanzione della nullità degli atti.

Successivamente, con il **decreto legge n. 148/2017**, convertito con legge n. 172/2017, il legislatore è intervenuto sulla disciplina dettata dal decreto legge n. 21/2012, estendendo l'esercizio dei poteri speciali applicabili nei settori dell'energia, delle comunicazioni e dei trasporti agli asset "ad alta intensità tecnologica" riferendosi, a titolo esemplificativo: 1) alle infrastrutture "critiche" o "sensibili", tra cui immagazzinamento e gestione dati e strutture finanziarie; 2) alle tecnologie "critiche", compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con potenziali applicazioni a doppio uso, la sicurezza in rete, la tecnologia spaziale o nucleare; 3) alla sicurezza dell'approvvigionamento di input "critici"; 4) all'accesso a informazioni "sensibili" o capacità di controllare le informazioni "sensibili".

Tale elencazione offre la misura dell'importanza dell'intervento; l'ampliamento del perimetro di azione ha determinato la valorizzazione dei poteri speciali ampliandone notevolmente il campo d'azione e rendendo certamente più difficoltosa la possibilità per gli operatori di prevedere le ipotesi – che secondo la disciplina previgente erano poche e facilmente verificabili (in particolare occorreva verificare che la società acquisenda o operasse nei settori della difesa militare e della sicurezza nazionale o possedesse uno dei pochi e puntualmente identificati asset nei settori dell'energia, dei trasporti e delle comunicazioni) – di soggezione ai poteri speciali del Governo. A ciò si aggiungono altre due importanti novità, ossia che la disciplina di cui al decreto legge n. 148 trova applicazione principalmente nel caso in cui l'acquisto a qualsiasi titolo di partecipazioni in società che detengono gli asset "strategici" avvenga da parte di un soggetto esterno all'Unione Europea e che il Governo può esercitare i poteri speciali non solo quando questo acquisto comporti una minaccia di grave pregiudizio agli interessi "essenziali" dello Stato (e, cioè, relativi alla sicurezza

e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti), ma anche quando esso possa minare la sicurezza o l'ordine pubblico.

4.2.2. Dal Decreto Brexit alla legge sul perimetro cibernetico. Lo stato della sicurezza informatica in Italia

Se questo era la cornice normativa nell'ambito della quale sono stati adottati numerosi DPCM attuativi, il **D.L. 25 marzo 2019, n. 22** (c.d. **Decreto Brexit**), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41, ha aggiunto all'ambito previsto dalla legge n. 56/2012 **l'art. 1 bis**, rubricato "Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G", con il quale sono stati inclusi, nelle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G. La nuova disposizione, in particolare, introducendo una chiara innovazione rispetto al regime generale precedente, prevede che:

1) il meccanismo di tutela dello Stato scatterà non solo nei casi di acquisizioni di partecipazioni azionarie, ma **anche nel caso di forniture di materiali e servizi**;
2) l'obbligo di notifica ai fini dell'esercizio del **potere di veto** o dell'i**mposizione di specifiche prescrizioni o condizioni**, riguarda la stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla **progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti 5G, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione**;
3) le operazioni sopra descritte sono sottoposte a notifica qualora poste in essere con "**soggetti esterni all'Unione Europea**" con ciò intendendo: a) qualsiasi persona fisica o persona giuridica, che non abbia la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale in uno Stato membro dell'Unione Europea o dello Spazio economico europeo o che non sia comunque ivi stabilito; b) qualsiasi persona giuridica che abbia stabilito la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione Europea o dello Spazio economico europeo o che sia comunque ivi stabilito, e che risulti controllato direttamente o indirettamente da una persona fisica o da una persona giuridica di cui al n. 1); c) qualsiasi persona fisica o persona giuridica che abbia stabilito la residenza, la dimora abituale, la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione Europea o dello Spazio economico europeo o che sia comunque ivi stabilito, al fine di eludere l'applicazione della disciplina in esame;

4) ai fini dell'esercizio dei poteri speciali, è prevista la valutazione anche degli "***elementi indicanti la presenza di fattori di vulnerabilità*** *che potrebbero compromettere* ***l'integrità e la sicurezza delle reti e dei dati*** *che vi transitano*".

Posta l'applicazione, alle ipotesi sub b), dei termini di cui al comma 4 del dl n. 21/2012, sopra descritti, l'art. 1 bis prevede la possibilità di adottare con DPCM misure di semplificazione delle modalità di notifica, dei termini e delle procedure relativi all'istruttoria per l'adozione del quale, la scorsa estate, è stata indetta una consultazione pubblica ad opera della Presidenza del Consiglio.

In ossequio al dettato normativo tracciato dal decreto Brexit, il Governo è stato chiamato a pronunciarsi sull'**accordo commerciale tra Fastweb ed il colosso tecnologico sudcoreano Samsung** per la progettazione, fornitura, configurazione e manutenzione di apparati software relativi alle componenti radio e core network per la realizzazione della rete 5G FWA nelle città pilota di Bolzano e Biella. Nel pronunciarsi su tale operazione, il Gruppo di Coordinamento che affianca la Presidenza del Consiglio nell'esercizio del *golden power*, ha adottato un decreto datato 26 giugno 2019[70].

I mesi successivi all'adozione del decreto Brexit hanno invece rappresentato una parentesi temporale che ha visto susseguirsi iniziative e ripensamenti da parte del Governo sulla disciplina da adottare per garantire la sicurezza delle reti 5G mediante applicazione della normativa sul *golden power*. E infatti, nel luglio 2019 il Governo ha varato il **decreto legge n. 64** con il quale si proponeva di integrare e modificare la disciplina contenuta nel decreto-legge n. 21/2012, mediante l'inserimento, tra l'altro, dell'art. 3 *bis* che modificava i termini di durata della procedura fissando in 10 giorni dalla conclusione di un contratto o accordo il termine per l'invio dell'informativa alla Presidenza del Consiglio dei Ministri, in 30 giorni, il termine entro cui soddisfare, ad opera delle imprese coinvolte, eventuali richieste di integrazione ed in 45 giorni – prorogabili una sola volta in

[70] Tale decreto, in particolare, ha fissato misure puntuali da osservare che si sostanziano, tra le altre, nell'effettuare test e verifiche ad opera di un soggetto terzo (riconosciuto dai soggetti istituzionali competenti) tesi a confermare l'inesistenza di interazioni funzionali tra le reti core e non virtuali della sperimentazione e l'attuale rete core di fastweb, l'adozione, da parte di quest'ultima, di misure di protezione e l'invio, alla Presidenza del Consiglio, degli esiti delle verifiche compiute sulla sicurezza al termine della sperimentazione, il coinvolgimento della funzione aziendale Security nei processi di governance relativi ad attività considerate strategiche alla luce del quadro normativo vigente, la trasmissione, entro 60 gg dall'adozione del decreto e successivamente ogni sei mesi, di una relazione descrittiva delle misure adottate per ottemperare a quanto prescritto dal decreto ed infine la tempestiva comunicazione di qualsiasi determinazione societaria o aziendale rilevante rispetto alle condizioni dettate dall'esecutivo nell'esercizio dei poteri speciali di cui lo stesso è titolare.

caso di particolare complessità – dalla notifica il termine entro cui il Presidente del Consiglio dei ministri avrebbe dovuto comunicare l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni e prevedeva un regime sanzionatorio specifico per le ipotesi di violazioni degli obblighi di notifica o delle prescrizioni impartite dall'Esecutivo nell'esercizio dei poteri speciali allo stesso spettanti.

Successivamente, il 21 settembre 2019 è stato varato il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, recante **disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.** Si tratta di un intervento di particolare rilevanza che all'art. 1 istituisce il perimetro di sicurezza nazionale cibernetica al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori (pubblici e privati aventi una sede nel territorio nazionale), da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. La medesima disposizione prevede l'adozione di due distinti DPCM, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), da sottoporre al parere delle Commissioni parlamentari competenti per materia (da rendere entro 30 gg.) e da aggiornare, secondo le procedure di seguito descritte, con cadenza almeno biennale: il primo, ai sensi del comma 2, da adottare entro **4 mesi** – introducendo una riduzione rispetto ai 6 previsti nel ddl – dalla data di entrata in vigore della legge di conversione (21 novembre 2019), su proposta del Comitato interministeriale per la sicurezza della Repubblica con il quale:

1) individuare **le amministrazioni pubbliche, gli enti e gli operatori inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti** sulla base di criteri che valutano se il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e se l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici secondo una logica di gradualità tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

2) **definire** – a opera dell'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri – **i criteri** con i quali i soggetti individuati predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. Quanto alla procedura di trasmissione di tali elenchi, la norma fissa in sei mesi dalla data di entrata in vigore del DPCM il termine per la trasmissione alla Presidenza del Consiglio ed al MiSE di tali elenchi che da questi ultimi vengono inoltrati al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Il secondo, da adottare entro **10 mesi** dall'entrata in vigore della legge di conversione del decreto legge, per: 1) la definizione delle procedure di notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano. Una volta ricevute le notifiche, la norma dispone il loro tempestivo inoltro, da parte del Gruppo di intervento, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica ed il successivo inoltro, da parte di quest'ultimo, all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato; 2) l'individuazione di misure – da parte di MiSE e Presidenza del Consiglio, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza – volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici relative alla struttura organizzativa preposta alla gestione della sicurezza, alle politiche di sicurezza e alla gestione del rischio, alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza, alla protezione fisica e logica e dei dati, all'integrità delle reti e dei sistemi informativi, alla gestione operativa, ivi compresa la continuità del servizio, al monitoraggio, test e controllo, alla formazione e consapevolezza ed all'affidamento di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale (di standard e di eventuali limiti).

La medesima disposizione, al comma 6, prevede l'adozione di un terzo regolamento, entro **dieci mesi** dalla data di entrata in vigore della legge di conversione del presente decreto, per la disciplina delle procedure, delle modalità ed i termini con i quali:

1) le **centrali di committenza che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici appartenenti a categorie individuate**, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto, **danno comunicazione di tale decisione al Centro di valutazione e certificazione nazionale** (CVCN), istituito presso il Ministero dello Sviluppo economico.

Il CVCN ha la facoltà, entro 45 gg. dalla ricezione della comunicazione (in caso di inutile decorso, si può procedere con la procedura di affidamento), prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, di effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con le centrali di committenza (e concludere entro 60 giorni), secondo un approccio gradualmente crescente nelle verifiche di sicurezza (nel caso di apposizione di condizioni o richieste di test i bandi devono contenere condizioni sospensive o risolutive collegate a quanto richiesto o apposto dal CVCN);

2) **i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano al CVCN la propria collaborazione** per l'effettuazione delle attività di test sostenendone gli oneri (il CVCN ha poteri di segnalazione rispetto all'eventuale mancata collaborazione al MISE, nel caso di forniture a soggetti privati ed alla Presidenza del Consiglio nel caso di soggetti pubblici)

Centrale il ruolo del CVCN al quale è rimessa l'elaborazione e l'adozione di schemi di certificazione cibernetica qualora quelli attualmente in forze non risultino adeguati ai fini di tutela del perimetro di sicurezza.

Se questo è il quadro normativo generale, con riferimento alle reti 5G, l'art. 4 *bis,* andando a riprendere e integrare le previsioni del decreto-legge n. 64 del 2019 decaduto, ha modificato il decreto legge n. 21 del 2012 in tema di poteri speciali del Governo nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, inserendo una serie di novità tra cui si segnalano, per rilevanza:

a) la **puntuale previsione degli elementi che il Governo deve considerare nella valutazione dell'acquirente** ed, in particolare, se l'acquirente sia direttamente o indirettamente controllato

dall'amministrazione pubblica, compresi organismi statali o forze armate, di un Paese non appartenente all'Unione Europea, anche attraverso l'assetto proprietario o finanziamenti consistenti, se l'acquirente sia già stato coinvolto in attività che incidono sulla sicurezza o sull'ordine pubblico in uno Stato membro dell'Unione Europea e se vi sia un grave rischio che l'acquirente intraprenda attività illegali o criminali;

b) le modifiche delle **modalità e delle tempistiche associate agli obblighi di notifica**: si prevede, nello specifico, la notifica alla Presidenza del Consiglio dei Ministri, entro dieci giorni dalla conclusione di un contratto o accordo, di un'informativa completa da parte dell'impresa che ha acquisito. È fissato in 30 giorni, prorogabile di 20 giorni e in caso di particolare complessità di ulteriori 20 giorni il termine per l'esercizio del potere di veto o l'imposizione di specifiche prescrizioni da parte del Presidente del Consiglio, rendendo il processo approvativo particolarmente lungo e complesso.

Risultano incisivi i i poteri del Presidente del Consiglio dei ministri. Quest'ultimo, infatti, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può disporre, ove indispensabile e per il tempo strettamente necessario all'eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

Nell'attesa – speriamo breve – che vengano adottati i decreti necessari per dare concreta attuazione al quadro normativo definito dal D.L. n. 105/2019, nel decreto-legge n. 23/2020 (c.d. "Decreto Liquidità Imprese"), in vigore dal 9 aprile, sono state inserite diposizioni che vanno ad incidere sul *golden power* da un lato, estendendolo a nuovi ambiti, dall'altro, rafforzandolo nelle modalità di esercizio. In particolare, gli artt. 15-17, al chiaro fine di evitare che, nell'ambito di una congiuntura economica sfavorevole come quella determinata dall'emergenza sanitaria in atto le imprese italiane di settori strategici possano essere acquistate all'estero a prezzi particolarmente ribassati, prevedono, fino alla data di entrata in vigore del primo dei DPCM sopra citati, l'estensione del *golden power* anche al settore alimentare, alla sanità, alle banche ed alle assicurazioni. Quanto al rafforzamento del *golden power*, le medesime disposizioni introducono la possibilità di avviare d'ufficio l'esercizio dei poteri speciali anche per operazioni non notificate e, in tal caso, al fine di raccogliere elementi utili, consentono al gruppo di coordinamento richiedere a pubbliche amministrazioni, enti pubblici o privati, imprese o altri soggetti terzi che ne siano in possesso, di

fornire informazioni e di esibire documenti ed alla Presidenza del Consiglio di stipulare convenzioni o protocolli di intesa con istituti o enti di ricerca.

4.2.3. L'iter di attuazione della disciplina sul perimetro di sicurezza: l'adozione del primo DPCM

Sebbene in ritardo rispetto alla tabella di marcia sopra delineata, complice, certamente, anche l'emergenza sanitaria ancora in atto, lo scorso 21 ottobre è stato pubblicato sulla Gazzetta Ufficiale il decreto del Presidente del Consiglio del Consiglio dei Ministri 30 luglio 2020, n. 131 che ha formalmente dato avvio all'articolata e complessa procedura di attuazione della disciplina del perimetro di sicurezza cibernetica. Si tratta del primo atto cui è affidato il compito, da un lato, di definire le **modalità e i criteri procedurali di individuazione dei soggetti** (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge e, dall'altro, declinare i **criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici** di rispettiva pertinenza, comprensivo della relativa architettura e componentistica.

Prima di procedere all'analisi delle disposizioni contenute nel decreto è interessante operare una sintetica rassegna dei principali rilievi formulati dal Consiglio di Stato nel parere del 21 maggio scorso. Il Consiglio di Stato, in particolare, ha espresso, a livello generale, il proprio timore che il percorso normativo tracciato dal D.L. 105/2019 per la costruzione del sistema del perimetro di sicurezza nazionale cibernetica, articolato in varie fasi e numerosi provvedimenti attuativi, possa determinare il rischio di generare un quadro regolatorio dispersivo e frammentato, segnalando la conseguente – e certamente condivisibile – esigenza di procedere alla redazione di un documento unitario, a fini conoscitivi e con efficacia meramente dichiarativa che rappresenti uno strumento utile per tutti gli operatori, pubblici e privati, coinvolti nell'esecuzione delle misure attuative del perimetro di sicurezza nazionale. A tale considerazione di carattere generale, il Consiglio di Stato ha affiancato numerosi commenti alle singole disposizioni che hanno riguardato la portata delle definizioni e l'esigenza di assicurare la piena conformità delle stesse con le altre già vigenti nel quadro normativo, la necessità di meglio precisare la durata delle fasi transitorie, nonché l'opportunità di prevedere che il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica (di cui si dirà *infra*), non previsto nel decreto legge n. 105/2019, disponga di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.

Anche le Camere – nello specifico la 1ª Commissione (Affari costituzionali) del Senato, le Commissioni riunite I (Affari costituzionali) e IX della Camera (Trasporti, Poste e Telecomunicazioni) e la V Commissione della Camera (Bilancio, Tesoro e Programmazione) – in esecuzione del dettato normativo, hanno espresso i rispettivi parerei rispettivamente in data 7, 8 e 15 luglio 2020, aderendo, da un lato, a molte delle considerazioni svolte dal Consiglio di Stato (tra cui quelle relative al Tavolo interministeriale) e, dall'altro, formulando specifici rilievi in merito, tra l'altro, alla necessità di ampliare l'alveo dei settori interessati per includere quello dell'Interno, quelli della salute, dell'acqua e della sicurezza alimentare, reti idriche, servizi alla persona e reti della trasportistica.

All'esito del rilascio di tali pareri è stato appunto finalizzato il testo del decreto oggetto di pubblicazione sulla G.U. il 20 ottobre scorso. Si tratta di un decreto che si compone di 12 articoli, divisi in quattro Capi, in cui innanzitutto vengono fornite una serie di importanti definizioni tra cui quella di "***pregiudizio per la sicurezza nazionale***", inteso come danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale serie e di "***analisi del rischio***", intendendo, in particolare, un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità, sulla sicurezza o sulla efficacia della funzione essenziale o del servizio essenziale, e conseguentemente, di trattare tale rischio individuando ed implementando idonee misure di sicurezza.

Molto rilevanti le definizioni tese all'individuazione, dal punto di vista tecnico, dell'ambito applicativo del decreto e, nello specifico, quella di **compromissione** ed **incidente**, nonché quella di **rete, sistema informativo, bene ICT ed architettura componentistica**.

Gli artt. 2 e 3 contribuiscono a delineare le modalità per **l'individuazione dei soggetti** inclusi nel perimetro oggetto del successivo Capo II, declinando i concetti di funzione e servizio essenziale. In particolare, in ossequio ai criteri generali fissati dal decreto legge, il decreto include nel concetto di **funzione essenziale** le attività tese ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia e la funzionalità dei

sistemi economico e finanziario, e dei trasporti. Rientrano, invece, nel concetto di **servizio essenziale**, i soggetti che svolgono attività: a) strumentali all'esercizio di funzioni essenziali dello Stato; b) necessarie per l'esercizio e il godimento dei diritti fondamentali; c) necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; d) ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Quanto ai **settori di attività** in cui operano i soggetti da inserire nel perimetro di sicurezza cibernetica, l'art. 3 del decreto, facendo salva l'estensione ad altri settori in sede di aggiornamento, aderendo agli stimoli formulati dalla Camere, individua i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro.

Il Capo II, nel fissare le modalità di individuazione dei soggetti inclusi nel perimetro di sicurezza cibernetica, definisce le modalità ed i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, attribuendo alle amministrazioni competenti il compito di: 1**) identificare le funzioni e servizi essenziali** – di diretta pertinenza o esercitati da soggetti vigilati o da operatori pubblici e privati – **che dipendono da reti, sistemi informativi o servizi informatici la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale**; 2) valutare, con riguardo agli **effetti di una interruzione della funzione o servizio essenziale**, estensione territoriale, numero e tipologia di utenti potenzialmente interessati, livelli di servizio garantiti e possibili ricadute economiche, mentre, in relazione agli **effetti della compromissione** dello svolgimento della funzione o servizio essenziale, le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati, con riferimento alla tipologia e quantità degli stessi, alla loro sensibilità e allo scopo cui sono destinati; 3) **valutare la possibile mitigazione** – rispetto all'interruzione o alla compromissione dello svolgimento della funzione o servizio essenziale – considerando il tempo necessario per ripristinare lo svolgimento in condizioni di sicurezza, tenendo altresì conto della possibilità che la funzione o il servizio essenziale possano essere assicurati con modalità prive di supporto informatizzato, anche temporaneamente, ovvero parzialmente da altri soggetti.

Le amministrazioni individuano, poi, le funzioni o servizi essenziali per i quali sulla base dei suddetti criteri e delle conseguenti valutazioni – in caso di interruzione o compromissione – "*il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime*" ed operano una graduazione in scala crescente. In fase di prima applicazione, sono individuati i soggetti titolari di tali funzioni o servizi per i quali un'interruzione delle relative attività comporterebbe il mancato svolgimento della funzione o del servizio. Le varie amministrazioni, all'esito delle descritte valutazioni, stilano un **elenco** di soggetti che viene trasmesso al CISR e al CSIR tecnico e poi formalizzato in un atto amministrativo, adottato e periodicamente aggiornato dal Presidente del Consiglio dei ministri, su proposta del CISR. È compito del **Dipartimento delle informazioni per la sicurezza (DIS)** darne comunicazione alle amministrazioni interessate.

L'art. 6 dispone, invece, l'istituzione di un **Tavolo interministeriale** per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR, presieduto da un vice direttore del DIS, composto da due rappresentanti di ciascuna amministrazione CISR, un rappresentante per ciascuna delle due agenzie di informazioni (Agenzia informazioni e sicurezza esterna – AISE e Agenzia informazioni e sicurezza interna – AISI) e due rappresentanti dei ministeri di volta in volta interessati che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare di cui almeno uno, in adesione ai rilievi espressi da Consiglio di Stato e Camere, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, che si riunisca periodicamente, e comunque almeno una volta ogni 6 mesi (senza alcun gettone di presenza, compenso o rimborso spese o altri emolumenti per la partecipazione alle riunioni).

Il Capo III detta, invece, i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici prescrivendo ai soggetti inclusi nel perimetro di individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale valutando, nello specifico, l'impatto di un incidente sul bene ICT (in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali) e la dipendenza con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione e predisporre ed aggiornare, con cadenza almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li

compongono. In fase di prima applicazione, il decreto circoscrive tali adempimenti ai beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi, con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

L'art. 9 fissa in sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco il termine per procedere alla trasmissione degli elenchi appena descritti alla Presidenza del Consiglio o al Ministero dello sviluppo economico (ai quali sono attribuiti poteri di ispezione e verifica) e prevede che tale trasmissione avvenga mediante una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al NSC, nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Il Capo IV, infine, detta le disposizioni transitorie e finali, disponendo che in attesa dell'adozione del DPCM previsto dal decreto legge, l'elencazione dei soggetti e gli elenchi comprensivi della descrizione dell'architettura e della componentistica, nonché dell'analisi del rischio, siano trattati, conservati e trasmessi con modalità idonee a garantirne la sicurezza, mediante misure tecniche e organizzative adeguate.

4.2.4. La proposta di DPR per l'attività di CVCN e CV

Il decreto legge istitutivo del perimetro di sicurezza cibernetica ha definito, come evidenziato nei paragrafi precedenti, anche ruolo ed organizzazione del Centro di Valutazione e Certificazione Nazionale (CVCN) a cui è demandato il compito di elaborare ed adottare schemi di certificazione cibernetica, valutare il rischio e verificare le condizioni di sicurezza nonché l'assenza di vulnerabilità e di contribuire all'elaborazione delle misure di sicurezza prevedendo lo stanziamento di fondi per assunzione di nuovo personale specifico. Il medesimo decreto, poi, nel tracciare i vari step che condurranno alla composizione e consentiranno l'operatività del perimetro di sicurezza nazionale cibernetica, ha previsto l'adozione di un regolamento (che avrebbe dovuto vedere la luce entro fine settembre 2020) con cui definire le modalità di svolgimento delle attività di *procurement* da parte dei soggetti inclusi nel perimetro cibernetico nazionale per quel che concerne l'acquisizione di beni e servizi informatici prevedendo che i soggetti afferenti al perimetro cibernetico nazionale che intendano acquisire beni, sistemi e servizi Ict, debbano darne comunicazione al CVCN il quale, per l'appunto, "*può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software*". Ebbene, il 3 agosto scorso è stato pubblicato il **bando pubblico** per la selezione di 70

esperti in sicurezza informatica che andranno, appunto, a costituire il CVCN, tassello fondamentale nel disegno generale tracciato dal decreto.

Mentre continua la procedura di selezione dei componenti il CVCN, nel frattempo è stato proposto uno **schema di regolamento** (al vaglio del Consiglio dei Ministri), indispensabile ai fini dell'operatività del CVCN, che in attuazione dell'art. 1 c. 6 del decreto istitutivo del perimetro, definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

La proposta si compone di 4 Capi che definiscono con puntualità le tipologie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN, le modalità ed i contenuti delle comunicazioni da effettuare in favore di CVCN o CV da parte dei soggetti inclusi nel perimetro, le tipologie di valutazioni, test e verifiche realizzabili, nonché le attività di verifica ed ispezione cui possono essere sottoposti i soggetti inclusi nel perimetro. In particolare, mentre il Capo I contiene le definizioni e definisce l'ambito applicativo del decreto, il Capo II disciplina minuziosamente la procedura di valutazione del CVCN e dei CV.
L'art. 3, in particolare, fissa contenuti e modalità di trasmissione della **comunicazione di affidamento** da parte dei soggetti inclusi nel perimetro nei confronti di CVCN o CV prevedendo, nello specifico, che essa avvenga per via telematica e che contenga le seguenti informazioni: a) la descrizione generale dell'oggetto di fornitura; b) l'impiego, ovvero destinazione d'uso dell'oggetto di fornitura nell'ambito dei beni ICT; c) la categoria di appartenenza dell'oggetto di fornitura; d) le informazioni e i servizi che l'oggetto di fornitura deve trattare e le relative modalità di gestione; e) le informazioni relative all'eventuale acquisizione mediante Consip SpA o i soggetti aggregatori. A ciò si aggiunge l'invio del **documento di analisi del rischio** associato all'oggetto della fornitura, anche in relazione all'ambito di impiego, nel quale indicare i componenti con i quali l'oggetto della fornitura interagisce e le configurazioni di tali componenti, le eventuali misure di sicurezza esistenti di tipo fisico, tecnico, procedurale, relative al personale con indicazione delle eventuali certificazioni o verifiche eseguite e i requisiti di sicurezza che caratterizzano l'impiego dell'oggetto

di fornitura, espressi in termini di capacità di proteggere la disponibilità, l'integrità e la riservatezza delle informazioni e dei servizi. Per quanto concerne le metodologie da seguire nella redazione di tale documento, lo schema demanda ad atto del CVCN da adottarsi entro 60 gg. dall'entrata in vigore del medesimo decreto.

L'art. 4, invece, entra nel vivo dell'attività valutativa di CVCN e CV, descrivendo il **procedimento di verifica e valutazione** dell'analisi documentale contenuta nella comunicazione, individuando le singole fasi ed i relativi termini. Nello specifico, la procedura si articola in: 1) verifiche preliminari, imposizione di condizioni e di test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, da compiersi entro il termine di quarantacinque giorni dalla comunicazione (prorogabile una sola volta di quindici giorni nei casi di particolare complessità ed in particolare, quando l'oggetto di valutazione è costituito da beni, sistemi e servizi ICT integrati tra di loro, è basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate o interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali); 2) fase di preparazione all'esecuzione dei test, esecuzione dei test di hardware e di software e definizione di eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro; 3) esecuzione dei test di hardware e di software e definizione di eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro (da concludersi entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV).

Lo schema, in una logica di semplificazione, prevede un meccanismo di **silenzio-assenso** per cui inutilmente decorsi i termini sopra indicati senza che CVCN o CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento e nell'esecuzione del contratto.
La medesima disposizione prevede la condivisione da parte di CVCN, con i CV e i Laboratori accreditati di prova, indipendente dai soggetti inclusi nel perimetro e dai fornitori, che ha ottenuto l'accreditamento dal CVCN (LAP), le metodologie per l'effettuazione dei test, di cui si prescrive di garantire la riservatezza.

Quanto all'**individuazione di condizioni e test**, l'art. 5 prescrive a CVCN e CV di tener conto, nell'individuazione dei test da eseguire, dell'analisi del rischio e dei livelli di severità, demandando l'individuazione test corrispondenti ai livelli di severità derivanti dall'analisi del rischio all'atto che il CVCN dovrà adottare entro 60 gg. dall'entrata in vigore di tale decreto. Quanto alle tipologie di

test richiedibili, si tratta di test di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto e test di intrusione a supporto dell'analisi di vulnerabilità.

Quanto al **fornitore**, nel caso di imposizione di test, lo schema prescrive l'esecuzione, da parte dello stesso, di una serie di attività propedeutiche e indispensabili alla loro esecuzione ed in particolare: a) fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza; b) provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il fornitore o presso il soggetto del perimetro; c) fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni; d) fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione; e) fornire una descrizione di test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

I successivi artt. 6 e 7 disciplinano la **fase di preparazione e realizzazione dei test** prescrivendo a CVCN e CV il compimento di specifiche attività di verifica tese ad evitare duplicazioni di test già eseguiti o in corso di esecuzione ed eventualmente integrare quanto già testato ed autorizzando il CVCN ad affidare l'esecuzione dei test ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore. All'esito dei test il CVCN, i CV e i LAP redigono un rapporto di prova nel quale sono indicati in dettaglio l'ambiente di test, le prove eseguite ed i relativi esiti. I LAP, eventualmente incaricati per l'esecuzione dei test, trasmettono il rapporto di prova al CVCN entro 7 giorni lavorativi dalla scadenza dei termini per l'esecuzione dei test. Sulla base del rapporto di prova, il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test e lo comunicano al soggetto incluso nel perimetro e al fornitore.
Il Capo IV, infine, individua l'oggetto delle **verifiche e** delle **ispezioni** di competenza di Presidenza del Consiglio e Ministero dello Sviluppo Economico dettando disposizioni di tipo organizzativo e procedurale e demandando, comunque, a tali autorità la redazione degli atti di programmazione sulla base dei quali disporre verifiche ed ispezioni.

P.A.

CONCLUSIONI

Il lockdown imposto dalle autorità pubbliche per contrastare la diffusione della pandemia ha messo in evidenza l'importanza assunta nella società moderna dalle reti di telecomunicazione. Per questo motivo, nonostante la rete nazionale abbia mostrato una notevole resilienza anche se sottoposta a stress difficilmente prevedibili a priori, è importante non rallentare lo sforzo in termini di investimenti, con un occhio al futuro, che nelle reti mobili non può che essere proiettato al 5G. La realizzazione delle reti di quinta generazione, come certificato da numerosi studi di impatto, costituisce un'importante opportunità di sviluppo e crescita a livello planetario, grazie soprattutto alla capacità di abilitare applicazioni avanzate (es. Internet delle cose, guida autonoma, telemedicina).

Risulta dunque fondamentale, soprattutto in questo momento nel quale si deve fronteggiare la peggiore crisi economica dal secondo Dopoguerra, incoraggiare gli **investimenti** degli operatori e ridurre al minimo gli impedimenti burocratici che rallentano il ***roll-out* delle nuove reti**. Secondo le previsioni del GSMA, infatti, l'**Europa** nel prossimo futuro rischia di rimanere indietro, rispetto a Cina e Stati Uniti, nella corsa alla realizzazione delle nuove reti, con un conseguente incremento del **gap di competitività** nelle tecnologie più avanzate delle economie del vecchio continente rispetto ai competitor globali. Come dimostrano i dati evidenziati nel presente studio, dopo l'impulso iniziale delle istituzioni e dei principali stakeholder europei, l'Europa registra già oggi un ritardo negli investimenti e nell'adozione del 5G, sia rispetto all'Asia che agli Stati Uniti. Un divario che è ancora possibile colmare ma solo con un'azione sufficientemente rapida e il più possibile coordinata a livello europeo.

Per assicurare all'Europa di essere all'avanguardia e competitiva, a livello globale, nello sviluppo del 5G, è infatti indispensabile, a livello normativo, adottare un **approccio comune** che garantisca la creazione di un ecosistema favorevole agli investimenti ed affronti, secondo una logica univoca, tutte le questioni in grado di condizionare il deployment del 5G, prima tra tutte, per rilevanza, la tematica della sicurezza. Rispetto a tale questione, in particolare, appare cruciale fissare obiettivi di armonizzazione, soprattutto rispetto a standard e certificazioni, quanto più possibile ambiziosi.

Anche in **Italia**, dove gli **investimenti necessari** nei prossimi 5 anni per la transizione al 5G sono stimati tra i €55 e i 75 miliardi, ovvero fino a 5 volte quelli sostenuti dagli operatori nel quinquennio appena trascorso, appare fondamentale trovare forme di incentivazione e rimozione delle barriere che come rilevato anche da analisi internazionali, gravano sul settore delle tlc, dai vincoli infrastrutturali a quelli relativi ai limiti elettromagnetici, fino alle recenti disposizioni delle autorità

locali che hanno bloccato le infrastrutturazioni con standard di nuova generazione. A tal proposito, molto rilevanti le disposizioni contenute nel **decreto Semplificazioni** (D.L. n. 76 del 16 luglio 2020), che ha tra l'altro introdotto il divieto per gli enti locali di introdurre limitazioni alla localizzazione in aree generalizzate del territorio di stazioni radio base per reti di comunicazioni elettroniche di qualsiasi tipologia e di incidere, anche in via indiretta o mediante provvedimenti contingibili e urgenti, sui limiti di esposizione a campi elettrici, magnetici ed elettromagnetici, nonché sui valori di attenzione e sugli obiettivi di qualità.

Se le iniziative intraprese sul piano della cantierabilità degli investimenti vanno nella direzione di introdurre forme di semplificazione delle procedure, quelle relative alla **sicurezza** dovrebbero muoversi coerentemente, per facilitare i progetti che rispondano a requisiti prestabiliti, anche molto stringenti, ma allo stesso tempo trasparenti e non discriminatori.
In questo contesto, le dinamiche di mercato si intrecciano inestricabilmente con quelle relative alla sicurezza, che hanno assunto una connotazione geopolitica scaturita nell'innalzamento dei vincoli per l'accesso al mercato da parte dei fornitori extra-europei di apparecchiature 5G, fino ad una vera e propria esclusione a priori praticata in alcuni Paesi, in particolare quelli che fanno capo ai *Five Eyes*.

Parallelamente, si osserva come l'upgrade al 5G sia oramai considerato un *must-have* per tutti gli operatori dei maggiori Paesi europei, e ogni singolo Stato stia studiando policy adeguate a garantirne lo sfruttamento delle potenzialità e dei vantaggi ad esso legati in termini economici, di occupazione, e di sviluppo. L'accesso al mercato per i fornitori di apparecchiature 5G è quindi divenuto un tema di grande rilevanza per gli assetti economici e geo-politici dei Paesi europei, collegati al Patto Atlantico, e di quelli extra-europei.

Se a livello generale, in una logica di promozione della competitività del sistema Europa, sarà cruciale garantire la definizione di standard e certificazioni comuni, ciascuno dei Paesi analizzati sta adottando politiche proprie, secondo logiche riconducibili essenzialmente a due principi: la necessità di non mettere a rischio la realizzabilità di progetti ritenuti essenziali per lo sviluppo delle nuove tecnologie e la tutela dei principi economici e commerciali praticati nel mondo occidentale.

Dalle tendenze e dai risultati relativi alla sottoscrizione degli **accordi di natura commerciale a livello mondiale**, si rileva come il mercato si mantenga piuttosto ristretto, e, con particolare riferimento all'Europa, la scelta sia confinata ad un numero esiguo di operatori in grado di soddisfare standard

e investimenti richiesti. Nella maggior parte dei casi, infatti, gli accordi per il 5G risultano essere siglati sulla base di rinnovi con i precedenti fornitori, in modo da garantire ottimizzazione dei costi e continuità di servizio. A tale proposito, esclusioni a priori all'ingresso di soggetti extraeuropei nello sviluppo e nella fornitura di prodotti e servizi relativi alle reti 5G, nonché l'innalzamento di altre possibili barriere d'ingresso in forma più o meno esplicita con un ristringimento dei perimetri cibernetici, rischiano di produrre esiti problematici per la competitività in un settore che già di per sé presenta limiti come quello delle telecomunicazioni in Europa. L'esclusione da futuri sviluppi tecnologici e dal dispiegamento delle reti 5G, insieme all'interruzione di contratti di forniture preesistenti, rischierebbero infatti di causare un innalzamento dei costi e una riduzione del servizio per i consumatori, comportando un sensibile ritardo nella diffusione delle nuove tecnologie digitali e nelle opportunità derivanti da un uso maggiore delle infrastrutture innovative.

Nel complesso, si osserva come allo stato attuale, i **tre fattori-chiave** emersi dall'analisi, ovvero mercato dell'offerta di apparecchiature 5G ristretto a 3-4 fornitori, necessità di compatibilità tra apparecchiature (e quindi fornitori) 4G e 5G, ed evoluzione delle normative tendente ad un'ulteriore restrizione del mercato dell'offerta per ragioni geopolitiche, determinino una situazione di stallo o rallentamento nelle operazioni di infrastrutturazione che rischia di avere a sua volta effettivi negativi in termini di minore sviluppo tecnologico e ritardati (e probabilmente anche minori) benefici economici derivanti dalla rivoluzione 5G. **Obiettivi di sicurezza e di competitività** non devono essere visti in una logica di *trade-off* che al momento attuale rischia di comportare sacrifici eccessivamente onerosi, dall'una e dall'altra parte. Occorre sforzarsi per trovare soluzioni che consentano di raggiungere gli uni e gli altri, essendo consapevoli naturalmente che non esiste un rischio zero in termini di sicurezza né un automatismo immediato in termini di benefici economici. Ma sforzandosi costruttivamente di individuare le soluzioni più robuste e lungimiranti che possano consentire ai diversi attori, pubblici e privati, di prepararsi al meglio alle sfide epocali che dovremo affrontare nei prossimi anni e decenni.

Tutto ciò dovrà avvenire nel contesto di un mercato delle telecomunicazioni e dell'ICT dove l'internazionalizzazione è progressivamente cresciuta nel corso degli ultimi decenni mostrando, nei casi in cui si è giunti a forme di standardizzazione internazionale dei requisiti e delle procedure relative alla sicurezza delle reti, la maggiore diffusione di reti e servizi e parallelamente dei benefici economici apportati da tali innovazioni. In questo contesto, molto interessante appaiono le operazioni condotte dai maggiori organismi di standardizzazione internazionale, l'ETSI, il 3GPP e GSMA. Questi ultimi, in particolare, sono al lavoro per implementare un **insieme di standard di**

sicurezza internazionale, chiamati **NESAS** e **SCAS**, che presenta molteplici vantaggi sia per i fornitori di apparecchiature e gli operatori di rete, sia per i singoli Stati. Tali standard possono essere il riferimento infatti per i fornitori per la certificazione dei propri prodotti e i singoli Stati membri che possono eventualmente integrarli con **ulteriori verifiche e/o certificazioni a livello nazionale**. Per questo ci pare che debba essere presa in seria considerazione l'adesione dell'Italia a tali forme condivise di regolazione della cyber sicurezza, in modo da affrontare congiuntamente la sfida tecnologica derivante dalla diffusione del 5G.

A ciò si aggiunge la necessità, **a livello nazionale**, di predisporre rapidamente e compiutamente un **set di strumenti normativi** in grado di creare un ecosistema improntato a quella chiarezza e certezza indispensabili ad assicurare uno sviluppo sicuro delle reti 5G.
A tale riguardo si segnalano **due esigenze concorrenti**: da un lato, assicurare che la complessa procedura disegnata dal D.L. n. 105/2019 per la definizione del perimetro di sicurezza nazionale cibernetica sia portata a compimento secondo tempistiche ragionevoli; dall'altro, che il mosaico normativo che si andrà man mano componendo con l'adozione dei diversi decreti e regolamenti si armonizzi con la vigente disciplina sul *golden power* per le reti 5G al fine di assicurare un set di norme quanto più possibile chiaro.

Quanto al **perimetro di sicurezza nazionale cibernetica** delineato dal decreto legge n. 105/2019, rispetto all'articolata e complessa procedura disegnata da tale decreto, il primo DPCM ha finalmente visto la luce con la pubblicazione in G.U. lo scorso 21 ottobre, mentre è ancora in fase embrionale lo schema di DPR che definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV).
Considerato il ritardo nell'adozione del primo DPCM, conseguente anche alla necessità di dover gestire un'emergenza sanitaria evidentemente improcrastinabile, e stante la necessità, per la rilevanza delle tematiche disciplinate, di affrontare compiutamente il dibattito sulle disposizioni di cui si compone lo schema, sarà cruciale la capacità del sistema Paese di finalizzare speditamente tutti gli atti indispensabili a disegnare il perimetro, a rendere operative le procedure di verifica che vedono come protagonisti **CVCN e CV** e a creare così quella certezza indispensabile per gli investimenti nelle reti 5G. Dotando il CVCN e i CV delle **risorse adeguate** per far fronte alle sfide particolarmente complesse per assicurare al contempo un obiettivo tecnologico sufficientemente ambizioso con un livello di sicurezza adeguato a proteggere l'Italia da minacce cibernetiche.

icom
sicurezza del 5G

icom
istituto per la competitività

Roma
Piazza dei Santi Apostoli 66
00187 Roma, Italia
Tel. +39 06 4740746

Bruxelles
Rond Point Schuman 6
1040 Bruxelles, Belgio
Tel. +32 (0) 22347882

info@i-com.it
www.i-com.it
www.icomRU.eu